Federal Office
for Information Security

Common Criteria Protection Profile

Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP]

BSI-CC-PP-0086

Document History

Version 1.01, May 20th, 2015	Final version	

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

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 Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP]
Editor/Sponsor:	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 1.01 as of May 20th, 2015
Registration:	BSI-CC-PP-0086
Keywords:	EAC2, eID-Application, eID-Card, PACE

1.2 TOE Overview

1.2.1 TOE Definition and Operational Usage

The Target of Evaluation (TOE) is a smartcard programmed according to [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). We mainly distinguish between two kinds of user data stored on the TOE:

1. *sensitive user data*. Such data are protected by Extended Access Control 2 (EAC2, cf. [TR03110-2]) and
2. *all other (common) user data*. Other data belonging to the user are protected by Password Authenticated Connection Establishment (PACE, cf. also [TR03110-2]). Note that EAC2 requires prior execution of PACE.

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

Applications considered in [TR03110-2] are an electronic passport (ePass) application, an electronic identity (eID) application, and a signature (eSign) application. This protection profile (PP) however does not make any assumptions on what kind of applications, and how many applications are included. If this protection profile is claimed by another protection profile or security-target (ST), a precise definition of applications including their data groups and protection levels should be given there. The combination of different applications for a product corresponds to loading different data into the EEPROM or flash memory of the smart card. Such a configuration of data groups yields a specific electronic document. Sets of, or requirements on configurations, and requirements on how the TOE is configured, i.e. how a configuration of data groups is loaded during manufacturing, should be defined by the ST writer.

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

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, and
4. the associated guidance documentation.

Application Note 1: 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, if a contactless chip is part of the TOE.

This PP claims strict conformance to [PACEPP]. There, slightly different terminology is used. For the ease of understanding, Table 1 gives a brief translation for the used terminology. Note that compound words that contain terminology of Table 1 should be translated by applying the translation on the relevant parts of the compound words. Since this is a syntactic change of terminology that does not impact any security related functionality, we do not give explicit justifications for needed refinements in Chapter 6.1.

This PP	**PACE PP**
electronic document	travel document
electronic document holder	travel document holder
electronic document presenter	traveler
sensitive user data	-
PACE terminal	BIS-PACE
common user data	user data
electronic document communication establishment authorization data	travel document communication establishment authorization data

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

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,
- 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, and
- its security functionality, and the data stored inside it, are self-protected.

1.2.3 TOE Type

The TOE type is a smartcard programmed according to [TR03110-2]. The smartcard contains multiple (at least one) applications. The programmed smartcard is called an electronic document as a whole.

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 personalization, i. e. linking the application data up to the electronic document holder.

Operational use of the TOE is explicitly in the focus of the current PP. 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 phases are considered to the extent that is required by the assurance package chosen here for the TOE; cf. chapter 6.3.3.

1.2.4 TOE Life Cycle

The life cycle of the TOE is the same as in [PACEPP] which consists of the following phases and steps:

Phase 1: Development

Step 1 Development of integrated circuit, the IC dedicated software and the guidance documentation

Step 2 Development of IC embedded software (operating system), the electronic document application(s) and the guidance documentation associated with these TOE components.

Phase 2: Manufacturing

Step 3 Production of integrated circuit

Step 4 (optional) Combining of IC with hardware for the contact based or contactless interface.

Step 5 Installation of embedded software, applications and pre-personalization data

Phase 3: Personalization of the Electronic Document

Step 6 Personalization of the Electronic Document

Phase 4: Operational Use

Step 7 Operational use

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 that supports contactless or contact-based communication according to [ISO14443], [ISO7816-4] and [ISO7816-2].

The TOE shall be able to distinguish the following kinds of terminals:

- *PACE terminal*. A PACE terminal is allowed to access (common) user data, but no sensitive user data.
- *EAC2 terminal*. Depending on its authorization level, an EAC2 terminal is allowed to access some or all sensitive user data.

The authorization level of an EAC2 terminal is determined by a certificate holder authorization template (CHAT), cf. [TR03110-2] and the SFR component FDP_ACF.1/TRM in Chapter 6.1.3.

Within this PP, the term *terminal* usually refers to any kind of terminal, if not explicitly mentioned otherwise. Different types of EAC2 terminals can exist. This PP does not make any assumptions on what kinds of terminals exist. If this PP is claimed, an overview should be given on which type of terminal is relevant for which application, and a security policy should be defined for the various types of EAC2 terminals by selection and/or assignment operations in the relevant components of the security functional requirements. Moreover, the PP/ST author should list and specify the types of EAC2 terminals in scope. Other terminals than PACE terminals and EAC2 terminals are out of scope of this PP.

2 Conformance Claims

2.1 CC Conformance Claim

90 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]
95 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012, [CC3]

as follows

Part 2 extended,

Part 3 conformant.

100 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 the Protection Profile

105 • Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA01, Version 1.01, 22.07.2014, [PACEPP].

2.3 Package Claim

The current PP is conformant to the following security requirements package:

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

2.4 Conformance Rationale

This PP claims strict conformance to [PACEPP], which has the following implications:

110 1. The TOE type of this PP is the same as the TOE type of the claimed PPs: The Target of Evaluation (TOE) is a smart card programmed according to [TR03110-2], and named an electronic document as a whole. Note that here the notion of a travel document is slightly extended to a more general 'electronic document', and [TR03110-2] replaces [ICAO9303]. Note that [TR03110-2] is downward compatible to [ICAO9303] however. This PP adds functionalities but also security mechanisms to
115 the TOE. These additions do not violate the security policy of the claimed PP.
2. The security problem definition (SPD) of this PP contains the SPD of the claimed PP. Hence, the SPD of this PP contains all threats, organizational security policies and assumptions of the claimed PP and identifies the additional threats T.Counterfeit/EAC2 (Counterfeit of electronic document chip data) and T.Sensitive_Data (Unauthorized access to sensitive user data).
120 3. The security objectives for the TOE in this PP include all security objectives for the TOE of the claimed PP and add the security objectives OT.AC_Pers_EAC2, OT.CA2, OT.RI_EAC2 and

OT.Sens_Data_EAC2. These mostly concern new functionalities of the TOE and require additional security measures.

4. The security objectives for the operational environment in this PP include all security objectives for the operational environment of the claimed PP, and add OE.Chip_Auth_Key, OE.RestrictedIdentity and OE.Terminal_Authentication. These only concern new functionalities (optional in the case of OE.RestrictedIdentity) of the TOE and do not violate the security policy of the claimed [PACEPP].

5. The security functional requirements (SFRs) specified in this PP include all SFRs specified in the claimed PP. Some SFRs are refined by either increasing the security requirements, or by adding rules for additional user data or functionalities of the TOE. The added SFRs concern additional user data or functionalities of the TOE, and do not violate the security policy of the [PACEPP].

6. The security assurance requirements (SARs) specified in this PP are the same as the SARs specified in the claimed PP.

2.5 Conformance Statement

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

3 Security Problem Definition

3.1 Introduction

3.1.1 Assets

3.1.1.1 Primary Assets

135 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

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.

140 *Generic Security Property:* Authenticity

This asset is equal to the one defined in [PACEPP].

Tracing Data

Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

145 *Generic Security Property:* Unavailability

This asset is equal to the one defined in [PACEPP]. Note that unavailability here is required for anonymity of the electronic document holder

Sensitive User Data

User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC2.

150 *Generic Security Properties:* Confidentiality, Integrity, Authenticity

User Data stored on the TOE

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be accessed either by a PACE terminal, or, in the case of sensitive data, by an EAC2 terminal with appropriate authorization level.

Generic Security Properties: Confidentiality, Integrity, Authenticity

155 This asset is an extension of the asset defined in [PACEPP].

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 an extension of the asset defined in [PACEPP]. As for confidentiality, note that even though not
160 each transferred data element represents a secret, [TR03110-2] requires confidentiality of all transferred data by secure messaging, employing the encrypt-then-authenticate approach.

All these primary assets represent user data in the sense of Common Criteria (CC).

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 of TOE Functions and Data only for Authorized Subjects

165 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 used for verification of the authorization
170 attempts as an authorized user (PACE password). These data are stored in the TOE and not send to it.

Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

Generic Security Properties: Confidentiality, Integrity

Secret Electronic Document Holder Authentication Data

175 Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (sent PACE passwords, e.g. PIN or CAN).

Generic Security Properties: Confidentiality, Integrity

TOE internal Non-Secret Cryptographic Material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality. An example for such non-secret material is the
180 document security object (SO_D) that contains a digital signature.

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

185 *Application Note* 2: Data for electronic document holder authentication and for authorization of communication with the electronic document can be categorized as (i) reference information that are persistently stored within the TOE, and (ii) verification information for the TOE that are input by a human user during an authentication and/or authorization attempt.
The TOE shall secure both reference information, and, together with the connected terminal, verifica-
190 tion information that are transferred in the channel between the TOE and the terminal.

Application Note 3: 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 as-

sumed to possess at most high attack potential. Note that the attacker might capture any subject role recog-
195 nized 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 coun-
200 tries 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 EAC2 terminals, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates,
205 see [TR03110-3].

Document Signer (DS)

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object (SO_D) that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificates, see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.

Document Verifier (DV)

210 An organization issuing terminal certificates. The DV is a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC2 terminals, see [TR03110-3].

Electronic Document Holder

A person who the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic document. Note that an electronic document holder can also be an attacker.

Electronic Document Presenter

215 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, cf. below.

Manufacturer

Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufac-
220 turer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.

PACE Terminal

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

Personalization Agent

225 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 activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic docu-

ment, (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.

EAC2 Terminal

A terminal that has successfully passed Terminal Authentication 2 is an EAC2 terminal. It is 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 that is neither a PACE terminal nor anEAC2 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.Counterfeit/EAC2 Counterfeit of electronic document chip data

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

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

Asset: authenticity of user data stored on the TOE

T.Sensitive_Data Unauthorized access to sensitive user data

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

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

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

This PP includes the following threats from [PACEPP]. Due to identical definitions and names, the definitions are not repeated here.

- **T.Abuse-Func**

- **T.Eavesdropping**
- **T.Forgery**
  Application Note 4: T.Forgery from [PACEPP] is extended here to all kinds of (PACE terminals and EAC2 terminals) targets that are outsmarted by the attacker.
- **T.Information_Leakage**
  Application Note 5: Confidential user data in T.Information_Leakage from [PACEPP] include sensitive user data defined in this PP.
- **T.Malfunction**
- **T.Phys-Tamper**
- **T.Skimming**
- **T.Tracing**

3.3 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSPs) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations, cf. [CC1].

P.EAC2_Terminal Abilities of Terminals executing EAC Version 2

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

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

If the TOE supports the Restricted Identity protocol, the electronic document issuer shall ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as defined in [TR03110-2]

P.Terminal_PKI PKI for Terminal Authentication

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

This PP includes the following organizational security policies from [PACEPP]:

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

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

3.4 Assumptions

This PP includes the assumption from [PACEPP], namely **A.Passive_Auth** and defines no further assumptions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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.AC_Pers_EAC2 Personalization of the Electronic Document

305 The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2.

Justification: This security objective for the TOE modifies OT.AC_Pers from [PACEPP] as the additional fea-
310 tures of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

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

The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [TR03110-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be pro-
315 tected against attacks with high attack potential.

OT.RI_EAC2 Support of Restricted Identity by the TOE

If the TOE supports pseudonymous authentication, it must use the Restricted Identity protocol as defined in [TR03110-2].

OT.Sens_Data_EAC2 Confidentiality of sensitive User Data

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

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

325 This PP includes the following security objectives for the TOE from [PACEPP]:

- **OT.Data_Authenticity**
  Application Note 6: OT.Data_Authenticity from [PACEPP] shall be extended to all kinds of PACE terminals and EAC2 terminals.
- **OT.Data_Confidentiality**
- 330 **OT.Data_Integrity**
  Application Note 7: OT.Data_Integrity from [PACEPP] is extended here to all kinds of PACE terminals and EAC2 terminals.
  Justification: Obviously, data integrity must be ensured w.r.t. all possible terminal types.
- **OT.Identification**
- 335 **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 as well.

4.2 Security Objectives for the Operational Environment

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

The electronic document issuer has to ensure that the electronic document's chip authentication key pair and the Restricted Identification key pair are generated securely, that the private keys of these key pairs are stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110-2] to check the authenticity of the electronic document's chip.

Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

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

If the TOE supports pseudonymous identification and thus implements the Restricted Identity protocol, the electronic document issuer has to ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as required according to [TR03110-2].

Justification: The TSF of [PACEPP] does not include any mechanism to identify the document holder by using a pseudonym. Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

OE.Terminal_Authentication Key pairs needed for Terminal Authentication

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

Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of the PACE password). Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

This PP includes the following security objectives for the TOE from [PACEPP]:

- **OE.Legislative_Compliance**
- **OE.Passive_Auth_Sign**
- **OE.Personalisation**
- **OE.Terminal**
  Application Note 8: Opposite to OE.Terminal from [PACEPP], a terminal supporting EAC2 according to [TR03110-2] needs to store its own credentials for Extended Access Control and (if used) the Restricted Identity.
- **OE.Travel_Document_Holder**

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

4.3 Security Objective Rationale

Table 2 provides an overview of the coverage of the security objectives. Threats and security objectives and policies that are imported verbatim from [PACEPP] are written in *cursive* style. Extended and new threats, security objectives and policies are written in standard style. Instead of copying verbatim text from [PACEPP], here only the rationale for new or altered threats and new or altered security objectives is given.

The threat **T.Counterfeit/EAC2** addresses the attack of an unauthorized copy or reproduction of the genuine electronic document. This attack is countered by the proof of the chip's authenticity, as aimed by OT.CA2 using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by OE.Chip_Auth_Key. According to OE.Chip_Auth_Key, the terminal has to perform the Chip Authentication 2 protocol to verify the authenticity of the electronic document's chip.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a PACE terminal or an EAC2 terminal in order to gain access to transferred user data. This threat is countered by the security objective OT.Data_Confidentiality through a trusted channel based on PACE Authentication, and by OT.Sens_Data_EAC2 demanding a trusted channel that is based on Chip Authentication 2.

The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of user data and/or TSF-Data stored on the TOE, and/or exchanged between the TOE and the terminal. In addition to the security objectives from [PACEPP] which counter this threat, the threat is also addressed by the refinement of OT.AC_Pers, here renamed OT.AC_Pers_EAC2.

The threat **T.Sensitive_Data** is countered by the TOE-Objective OT.Sens_Data_EAC2, that requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during transmission. The objective OE.Terminal_Authentication requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the EAC2 terminal.

The threat **T.Skimming** addresses accessing the user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact-based interface. Additionally to the security objectives from [PACEPP] which counter this threat, the threat is also addressed by OT.Sens_Data_EAC2 that demands a trusted channel based on Chip Authentication 2, and requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Moreover, OE.Terminal_Authentication requires the electronic document issuer to provide the corresponding PKI.

The OSP **P.EAC2_Terminal** addresses the requirement for EAC2 terminals to implement the terminal parts of the protocols needed to executed EAC2 according to its specification in [TR03110-2], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by OE.Chip_Auth_Key which requires Chip Authentication and Restricted Identity keys to be correctly generated and stored, by OE.Terminal_Authentication for the PKI needed for Terminal Authentication, and by OE.Terminal which covers the PACE protocol and the Passive Authentication protocol.

	OT.Identification	OT.AC_Pers_EAC2	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*	OT.CA2	OT.RI_EAC2	OT.Sens_Data_EAC2	*OE.Personalisation*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*	OE.Chip_Auth_Key	OE.RestrictedIdentity	OE.Terminal_Authentication
T.Skimming			x	x	x								x								x
T.Eavesdropping					x								x								
T.Tracing						x											x				
T.Forgery		x	x	x			x		x					x	x	x					
T.Abuse-Func							x														
T.Information_Leakage								x													
T.Phys-Tamper									x												
T.Malfunction										x											
T.Counterfeit/EAC2											x								x		
T.Sensitive_Data													x								x
P.Manufact	x																				
P.Pre-Operational	x	x												x				x			
P.Terminal																x					
P.Card_PKI															x						
P.Trustworthy_PKI															x						
A.Passive_Auth															x						
P.EAC2_Terminal																x			x		x
P.RestrictedIdentity												x								x	
P.Terminal_PKI																					x

Table 2: Security Objective Rationale

405

P.Pre-Operational is enforced by security objectives from [PACEPP] that counter this OSP. In addition, the threat is also addressed by the refinement of OT.AC_Pers named OT.AC_Pers_EAC2.

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

410 The OSP **P.RestrictedIdentity** defines requirements on the generation and storage of the key pair(s) for the Restricted Identity protocol. This OSP is addressed by the objective OE.RestrictedIdentity w.r.t. to generation and storage of key pair(s) outside of the TOE. W.r.t. generation, storage and protection within the TOE, this OSP is addressed by the OT.RI_EAC2.

5 Extended Components Definition

415 This PP includes all extended components from the claimed PP [PACEPP]. This includes

- FAU_SAS.1 from the family FAU_SAS
- FCS_RND.1 from the family FCS_RND
- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM
- FPT_EMS.1 from the family FPT_EMS

420 For precise definitions of these components we refer to [PACEPP].

5.1 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE, the family FIA_API of the class FIA (Identification and authentication) is defined here. This family describes the functional requirements for proof of the claimed identity for the authentication verification by an external entity, where the other families of the class FIA address the verification of the identity of an external entity.

425 *Application Note* 9: Other families of the class FIA describe only the authentication verification of the user's identity performed by the TOE and do not describe the functionality of the TOE to prove its own identity. The following paragraph defines the family FIA_API in the style of Common Criteria part 2 (cf. [3], chapter 'Extended components definition (APE_ECD)') from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:

FIA_API.1 Authentication Proof of Identity.

Management FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to:

435 No other components

Dependencies:

No dependencies

FIA_API.1.1

The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorised user or role, or of the TOE itself*].

6 Security Requirements

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.

CC 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 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. 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 by underlining. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*. In some cases, the assignment made by the PP author 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 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.

6.1 Security Functional Requirements

This PP of course includes all components from claimed PPs. Sometimes, a claimed component applies to newly added components whereas the applied operations do not change. Consider for example FCS_CKM.4, which requires the destruction of all session keys. Session keys in the claimed PP - [PACEPP] - need only be destroyed after executing the PACE protocol, but here destruction must additionally be ensured after execution of Chip Authentication 2. Since nothing in the definition of the component FCS_CKM.4 changes, an iteration of this component in this PP would lead to a definition that is the same as the definition in [PACEPP] word-by-word. Thus the iteration operator is not appropriate. In such a case, we refrain from copying the definition, but just reference and explicitly remark the newly added scope, usually in an *Application Note*.

If applicable, for iterated components we explicitly point out relations among the iterations.

6.1.1 Class FCS

FCS_CKM.1/DH_PACE Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys

Hierarchical to:
No other components

Dependencies:
[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
not fulfilled, but **justified:**
A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
FCS_CKM.4 Cryptographic key destruction
fulfilled by FCS_CKM.4

FCS_CKM.1.1/DH_PACE
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *Diffie-Hellman-Protocol compliant to [PKCS3], ECDH compliant to [TR03111]*][2] and specified cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [**TR03110-2**][3].

Application Note 10: In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is changed to [TR03110-2], whereas [PACEPP] references [ICAO-SAC]. The difference between the two definitions is that [TR03110-2] defines additional optional parameters for the command MSE:Set AT. This optional parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2 (TA2) can be executed right after PACE (see FIA_UID.1/EAC2_Terminal). As [ICAO-SAC] does not consider TA2, no such definition is given there. These additional parameters are optional and not used during PACE itself (only afterwards). If PACE is run without TA2 afterwards, access to data on the chip is given as specified by [PACEPP]. If TA2 is run afterwards, access to data on the chip can be further restricted w.r.t. to the authorization level of the terminal. Therefore this change of references does not violate strict conformance to [PACEPP]. We treat this change of references as a refinement operation, and thus mark the changed reference using **bold** text.

Application Note 11: National cryptographic requirements may further restrict available choices in the selection of the above SFR.

Application Note 12: [PACEPP] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to implement Chip Authentication 2 (cf. FIA_API.1/CA), here FCS_CKM.1/DH_PACE applies for CA2 as well.

FCS_COP.1/SHA Cryptographic operation – Hash for key derivation

Hierarchical to:
No other components.

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
not fulfilled, but **justified:**
A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.
FCS_CKM.4 Cryptographic key destruction
not fulfilled, but **justified:**

2 [assignment*: cryptographic key generation algorithm*]
3 [assignment: *list of standards*]

A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.

FCS_COP.1.1/SHA

The TSF shall perform hashing[4] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes none[5] that meet the following: [FIPS180-4][6].

Application Note 13: For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function SHA-1 shall be used ([TR03110-3]). The TOE shall implement as hash functions either SHA-1 or SHA-224 or SHA-256 for Terminal Authentication 2, cf. [TR03110-3].
Within the normative Appendix of [TR03110-3] 'Key Derivation Function', it is stated that the hash function SHA-1 shall be used for deriving 128-bit AES keys, whereas SHA-256 shall be used for deriving 192-bit and 256-bit AES keys.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
not fulfilled, but **justified:**
The root key PK_{CVCA} (initialization data) used for verifying the DV Certificate is stored in the TOE during its personalization in the card issuing life cycle phase[7]. Since importing the respective certificates (Terminal Certificate, DV Certificate) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the current PP does not contain any dedicated requirement like FDP_ITC.2 for the import function.
FCS_CKM.4 Cryptographic key destruction
not fulfilled, but **justified:**
Cryptographic keys used for the purpose of the current SFR (PK_{PCD}, PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret, and hence need not to be destroyed.

FCS_COP.1.1/SIG_VER

The TSF shall perform digital signature verification[8] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 14: This SFR is concerned with Terminal Authentication 2, cf. [TR03110-2].

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

Hierarchical to:

No other components.

Dependencies:

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

4 [assignment: *list of cryptographic operations*]
5 [assignment: *cryptographic key sizes*]
6 [assignment: *list of standards*]
7 as already mentioned, operational use of the TOE is explicitly in focus of the current PP
8 [assignment: *list of cryptographic operations*]

FCS_COP.1.1/PACE_ENC

The TSF shall perform secure messaging – encryption and decryption[9] in accordance with a specified cryptographic algorithm AES in CBC mode[10] and cryptographic key sizes [selection: *128, 192, 256 bit*] that meet the following: [**TR03110-3**][11].

Application Note 15: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol (PACE-K_{Enc}) or Chip Authentication 2 (CA-K_{Enc}) according to FCS_CKM.1/DH_PACE . Note that in accordance with [TR03110-3], 3DES could be used in CBC mode for secure messaging. Due to the fact that 3DES is not recommended any more (cf. [TR03116-2]), 3DES in any mode is no longer applicable here. The PP/ST writer has to fill in appropriate – as specified in [TR03110-3] – key sizes for AES.

Application Note 16: Refinement of FCS_COP.1.1/PACE_ENC, since here PACE must adhere to [TR03110-3]. All references (both the one in [PACEPP] and [TR03110-3]) itself reference [ISO7816-4] for secure messaging. [TR03110-3] however further restricts the available choice of key-sizes and algorithms. Hence, [TR03110-3] is fully (backward) compatible to the reference given in [PACEPP].

FCS_COP.1/PACE_MAC Cryptographic operation – CMAC

Hierarchical to:
No other components.

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

FCS_COP.1.1/PACE_MAC

The TSF shall perform secure messaging – message authentication code[12] in accordance with a specified cryptographic algorithm CMAC[13] and cryptographic key sizes [selection: ~~*112*~~ *128, 192, 256 bit*] that meet the following: [**TR03110-3**][14].

Application Note 17: see Application Note 16.

Application Note 18: This SFR removes 3DES and restricts to CMAC compared to the SFR of [PACEPP] by selection. Hence, a minimum key-size of 128 bit is required.

In addition, this PP includes all remaining SFRs of [PACEPP]. For the class FCS, these are the following components:

- **FCS_CKM.4**
  The *Application Note* in [PACEPP] concerning this component requires the destruction of PACE session keys after detection of an error in a received command by verification of the MAC. While the definition of FCS_CKM.4 remains unaltered, here this component also requires the destruction of sessions keys after a successful run of Chip Authentication 2. The TOE shall destroy the CA2 session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.
- **FCS_RND.1**
  The *Application Note* in [PACEPP] concerning this component requires the TOE to generate random

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

numbers (random nonces) for PACE. While the definition of FCS_RND.1 remains unaltered, here this component requires the TOE to generate random numbers (random nonce) for all authentication protocols (i.e. PACE, CA2), as required by FIA_UAU.4.

6.1.2 Class FIA

For the ease of presentation, we give an overview of the used authentication mechanisms and directly corresponding SFRs.

PACE Protocol

FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/PACE
as required by FCS_CKM.1/DH_PACE

Terminal Authentication Protocol Version 2

FIA_UAU.1/EAC2_Terminal, FIA_UAU.5/PACE
as required by FCS_COP.1/SIG_VER

Chip Authentication Protocol Version 2

FIA_API.1/CA, FIA_UAU.5/PACE, FIA_UAU.6/CA
as required by FCS_CKM.1/DH_PACE

FIA_AFL.1/Suspend_PIN Authentication failure handling – Suspending PIN

Hierarchical to:
No other components.

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

FIA_AFL.1.1/Suspend_PIN
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE[15].

FIA_AFL.1.2/Suspend_PIN
When the defined number of unsuccessful authentication attempts has been met[16], the TSF shall suspend the reference value of the PIN according to [TR03110-2][17].

Application Note 19: This SFR is not in conflict to FIA_AFL.1 from [PACEPP], since it just adds a requirement specific to the case where the PIN is the shared password. Thus the assigned integer number for unsuccessful authentication attempts with any PACE password could be different to the integer for the case when using a PIN.

FIA_AFL.1/Block_PIN Authentication failure handling – Blocking PIN

Hierarchical to:
No other components.

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

15 [assignment: *list of authentication events*]
16 [selection: *met , surpassed*]
17 [assignment: *list of actions*]

FIA_AFL.1.1/Block_PIN

The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended[18] PIN as the shared password for PACE[19].

FIA_AFL.1.2/Block_PIN

When the defined number of unsuccessful authentication attempts has been met[20], the TSF shall block the reference value of PIN according to [TR03110-2][21].

FIA_API.1/CA Authentication Proof of Identity

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/CA

The TSF shall provide the protocol Chip Authentication 2 according to [TR03110-2][22], to prove the identity of the TOE[23].

FIA_API.1/RI Authentication Proof of Identity

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/RI

The TSF shall provide the Restricted Identification protocol according to [TR03110-2][24], to prove the identity of the TOE[25].

Application Note 20: Restricted Identification provides a sector-specific identifier of every electronic document. It thus provides a pseudonymous way to identify the electronic document holder in a case where the CHAT of the terminal does not allow to access sensitive user data that directly identify the electronic document holder. Restricted Identification shall only be used after successfully running Terminal Authentication 2 and Chip Authentication 2. Note that Restricted Identification is optional according to [TR03110-2], and thus the above SFR only applies if Restricted Identification is supported by the TOE.

FIA_UID.1/PACE Timing of identification

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/PACE

The TSF shall allow

18 as required by FIA_AFL.1/Suspend_PIN
19 [assignment: *list of authentication events*]
20 [selection: *met , surpassed*]
21 [assignment: *list of actions*]
22 [assignment: *authentication mechanism*]
23 [assignment: *authorised user or role, or of the TOE itself*]
24 [assignment: *authentication mechanism*]
25 [assignment: authorized *user or role*]

1. to establish a communication channel,
2. carrying out the PACE protocol according to [**TR03110-2**]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[26]
4. [assignment: *list of TSF-mediated actions*]

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

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

Application Note 21: The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK were used for PACE, the user identified is the electronic document holder using a PACE terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the electronic document holder itself, an authorized person other than the electronic document holder, or a device.

FIA_UID.1/EAC2_Terminal Timing of identification

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_UID.1.1/EAC2_Terminal
The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. carrying out the Terminal Authentication protocol 2 according to [TR03110-2][27]
5. [assignment: *list of TSF-mediated actions*]

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

FIA_UID.1.2/EAC2_Terminal
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 22: The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2 terminals are application dependent;

Application Note 23: In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE. The manufacturer writes the initialization data and/or pre-personalization data in the audit records of the IC.
Note that a personalization agent acts on behalf of the electronic document issuer under his and the CSCA's and DS's policies. Hence, they define authentication procedures for personalization agents. The TOE must functionally support these authentication procedures. These procedures are subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role personalization agent, if a terminal proves the respective Terminal Authorization level (e. g. a privileged terminal, cf. [TR03110-2]).

26 [assignment: *list of TSF-mediated actions*]
27 [assignment: *list of TSF-mediated actions*]

FIA_UAU.1/PACE Timing of authentication

Hierarchical to:
No other components.

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

665 FIA_UAU.1.1/PACE

The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to [**TR03110-2**]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[28]
670 4. [assignment: *list of TSF-mediated actions*]

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

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

Application Note 24: If PACE has been successfully performed, secure messaging is started using the derived
675 session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE. Application Note 23 also applies here.

FIA_UAU.1/EAC2_Terminal Timing of authentication

Hierarchical to:
No other components.

Dependencies:
FIA_UID.1 Timing of identification
fulfilled by FIA_UID.1/EAC2_Terminal

FIA_UAU.1.1/EAC2_Terminal
The TSF shall allow

680 1. to establish a communication channel,
2. carrying out the PACE protocol according to [TR03110-2],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. carrying out the Terminal Authentication 2 protocol according to [TR03110-2][29]

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

FIA_UAU.1.2/EAC2_Terminal
685 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 25: The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated terminal will immediately perform Chip Authentication 2 as required by FIA_API.1/CA using, amongst other, Comp(ephem-PK_{PCD}-TA) from the accomplished TA2. Note that Passive Authentication
690 using SO_C is considered to be part of CA2 within this PP.

28 [assignment: *list of TSF-mediated actions*]
29 [assignment: *list of TSF mediated actions*]

FIA_UAU.4/PACE Single-use authentication of the Terminals by the TOE

Hierarchical to:
No other components.

Dependencies:
No dependencies.

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

1. PACE protocol according to [**TR03110-2**],
2. Authentication Mechanism based on [selection: ~~*Triple-DES*~~, *AES or other approved algorithms*]
3. Terminal Authentication 2 protocol according to [TR03110-2][30].
4. [assignment: *identified authentication mechanism(s)*]

Application Note 26: For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The current PP supports a key derivation function based on AES; see [TR03110-2]. For TA2, the TOE randomly selects a nonce r_{PICC} of 64 bit length, see [TR03110-2]. This SFR extends FIA_UAU.4/PACE from [PACEPP] by assigning the authentication mechanism Terminal Authentication 2.

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_UAU.5.1/PACE
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*][31]
5. Terminal Authentication 2 protocol according to [TR03110-2],
6. Chip Authentication 2 according to [TR03110-2][32][33]
7. [assignment: *list of multiple authentication mechanisms*]

to support user authentication.

FIA_UAU.5.2/PACE
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)*]

30 [assignment: *identified authentication mechanism*(s)]
31 restricting the [selection: *Triple-DES, AES or other approved algorithms*]
32 Passive Authentication using SO_C is considered to be part of CA2 within this PP.
33 [assignment: *list of multiple authentication mechanisms*]

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[34].
5. [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Application Note 27: Refinement of FIA_UAU.5.2/PACE, since here PACE must adhere to [TR03110-2] and [TR03110-3], cf. *Application Note 10*.
Since the formulation "MAC-ENC mode" is slightly ambiguous (there is only one secure messaging mode relevant both in [PACEPP] and here, and it is actually the same in both references), it is removed here by refinement in the third bullet point of FIA_UAU.5.1.

Remark: Note that 5. and 6. in FIA_UAU.5.1/PACE and 3. and 4. of FIA_UAU.5.2/PACE are additional assignments (using the open assignment operation) compared to [PACEPP].

FIA_UAU.6/CA Re-authenticating of Terminal by the TOE

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FIA_UAU.6.1/CA
The TSF shall re-authenticate the user under the conditions each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal[35].

In addition, this PP includes all remaining SFRs of the claimed [PACEPP]/Class FIA:

- **FIA_AFL.1/PACE**
  Note here, in addition to the MRZ, the PACE password could also be a CAN or the PIN.
- **FIA_UAU.6/PACE**

6.1.3 Class FDP

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

Hierarchical to:
No other components.

Dependencies:

FDP_ACC.1 Subset access control
fulfilled by FDP_ACC.1/TRM
FMT_MSA.3 Static attribute initialization
not fulfilled, but **justified:**
The access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

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

FDP_ACF.1.1/TRM

The TSF shall enforce the Access Control SFP[36] to objects based on the following:

1) Subjects:
   a) Terminal,
   b) **PACE terminal**[37],
   c) EAC2 terminal [assignment: *list of EAC2 terminal types*];[38]
2) Objects:
   a) **all user data stored in the TOE; including sensitive user data.**[39]
   b) all TOE intrinsic secret (i.e. cryptographic) data.[40]
3) Security attributes:
   a) **Terminal Authorization Level (access rights)**[41][42]
4) [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2/TRM

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
A **PACE terminal** is allowed to read data objects from FDP_ACF.1/TRM after successful PACE authentication according to [**TR03110-2**], as required by FIA_UAU.1/PACE.[43]

FDP_ACF.1.3/TRM

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.[44]

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** is not allowed to read, to write, to modify, or to use any user data stored on the **electronic document**.
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the **electronic document**.
3. No subject is allowed to read "Communication Establishment Authorization Data' stored on the electronic document[45]

36 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]] (using the open assignment from [PACEPP])
37 equivalent to BIS-PACE, cf. Table1. Also renamed in the following.
38 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
39 we distinguish here between sensitive user data, and (common) user data. Data groups EF.DG3 and EF.DG4 as defined in FDP_ACF.1/TRM from [PACEPP] are considered sensitive user data, whereas all other data groups are considered user data here. Note that this mere renaming does not conflict with strict compliance to [PACEPP].
40 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
41 renamed from 'Authentication status of terminals' in [PACEPP], since the access controls here allow for a more fine-grained access compared to [PACEPP].
42 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
43 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
44 [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
45 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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.

6. Reading, modifying, writing, or using sensitive user data is only allowed 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[46].

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

Application Note 28: The above definition covers FDP_ACF.1.1/TRM from [PACEPP] and extends it by additional subjects and objects. Below we justify all refinements:
In FDP_ACF.1 1b) a *refinement* is used to replace the term BIS-PACE with PACE-Terminal as specified in Table 1. Such syntactic change does not violate strict conformance. Subject 1c) is added by applying the open assignment operation (4) from [PACEPP]. Next, data objects 2a), b) and c) of [PACEPP] are here generalized from a specific enumeration to *all user data stored on the TOE* as bullet point 2a) above using a refinement. Since this includes all data defined in [PACEPP] (DG3 and DG4 are sensitive data; the other DG's of [PACEPP] are common user data), this does not violate strict conformance. For 2b) in this PP the open assignment (4) of [PACEPP] is used to add an additional object.
The term *authentication status of terminals* (3a) is here *refined* to *terminal authentication level*, since the former term is simply very imprecise for a TOE implementing Terminal Authentication.
In FDP_ACF.1.2/TRM, besides the aforementioned renaming of terminology (a simple syntactic change without changing semantics), a reference is changed. For that reference, Application Note 10 applies.
For FDP_ACF.1.4/TRM rule 1, a slight refinement of wording ("not being" vs "being not") is made to increase clarity, and terms are replaced according to Table 1. This is however again just a syntactic correction without changing the semantics. In addition, the subject EAC2-Terminal is added. Since an EAC2-Terminal must be authenticated by executing PACE prior to be given access, this does not decrease security and thus is in conformance with [PACEPP]. Rule 2 is refined by applying Table 1. This syntactic replacement of terminology does also not violate strict conformance. The remaining rules 4-7 are additional assignments using the open assignment operation from [PACEPP]. Note that rule 4) narrows down the open assignment ([CC1], 8.1.2 c) of [PACEPP] by leaving itself an open assignment of PIN management rules.

Application Note 29: Note that here, all sensitive user data are assumed to be protected by EAC2 (cf. FIA_UAU.5). If this PP is claimed, the definition of sensitive user data may distinguish between different kinds of sensitive user data, where some are protected by EAC2, and some are protected by an equivalent (in terms of the security level) security mechanism, such as EAC1.

FDP_RIP.1 Subset residual information protection

Hierarchical to:
No other components.

46 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*] (rules 4-7)

Dependencies:
No dependencies.

FDP_RIP.1.1
The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects:

1. Session keys (**PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc})** (immediately after closing related communication session),
2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret *K*),
3. secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more)[47],
4. [assignment: *list of objects*].

Application Note 30: The functional family FDP_RIP possesses such a general character, that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-Data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric (*any previous information content of a resource is made unavailable*) for key destruction in addition to FCS_CKM.4/PACEPP that merely requires to ensure key destruction according to a method/standard.

In addition, this PP includes all remaining SFRs of the claimed PP [PACEPP]/Class FDP:

- **FDP_ACC.1/TRM**
  Note that "user data" as defined in FDP_ACC.1/TRM here includes both common and sensitive user data. For the access control SFP, see FDP_ACF.1/TRM (defined in this PP).
- **FDP_UCT.1/TRM**
- **FDP_UIT.1/TRM**

6.1.4 Class FTP

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

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FTP_ITC.1.1/PACE
The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **a PACE 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 PACE protocol according to [TR03110-2].**

FTP_ITC.1.2/PACE
The TSF shall permit ~~another trusted IT product~~ **a PACE terminal** [48] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE
The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and **a PACE terminal after PACE.** [49]

47 [assignment: *list of objects*]
48 [selection: *the TSF, another trusted IT product*]
49 [assignment: *list of functions for which a trusted channel is required*]

Application Note 31: The above definition refines FTP_ITC.1 from [PACEPP]. The definitions there are unclear as to what the "other trusted IT product" actually is. Since we distinguish here between trusted channels that are established once after PACE, and then then (re)established after CA2, the above refinement is necessary for clarification.

FTP_ITC.1/CA2 Inter-TSF trusted channel after CA2

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/CA2

The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **The trusted channel shall be established by performing the CA2 protocol according to [TR03110-2].**

FTP_ITC.1.2/CA2

The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal** [50] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2

The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2. [51]

Application Note 32: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE), the TA2 protocol (FIA_UAU.1/EAC2_Terminal) and the CA2 protocol (FIA_API.1/CA). If Chip Authentication 2 was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc})[52]. This secure messaging enforces the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

6.1.5 Class FAU

No new SFRs are included here, but this PP contains all SFRs of the claimed PP [PACEPP].

- **FAU_SAS.1**

6.1.6 Class FMT

FMT_SMF.1 Specification of Management Functions

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_SMF.1.1

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

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

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

52 otherwise secure messaging is continued using the established PACE session keys, cf. FTP_ITC.1/PACE

1. Initialization,
2. Pre-Personalization,
3. Personalization,
4. Configuration,
5. **Resume and unblock the PIN (if any),**
6. **Activate and deactivate the PIN (if any)**[53].

Application Note 33: The capability of PIN management gives additional security to the TOE.

Application Note 34: The SFR is here refined by including mechanisms for PIN management. A TOE without PIN management functionality can only use a commonly shared secret (such as the MRZ – in the case of an ID document – or the CAN) during execution of PACE to control access to sensitive information. A PIN however must not be shared and thus can be kept secret by the user. Hence, this refinement of FMT_SMF.1 increases protection of user data by allowing PIN access, and thus does not violate strict conformity to [PACEPP].

FMT_SMR.1/PACE Security roles

Hierarchical to:
No other components.

Dependencies:
FIA_UID.1 Timing of identification:
fulfilled by FIA_UID.1/PACE, FIA_UID.1/EAC2_Terminal, see also the *Application Note* below.

FMT_SMR.1.1/PACE
The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal,
4. **PACE terminal**,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. EAC2 terminal [*assignment: list of EAC2 terminal types*],
8. Electronic document holder[54],
9. [assignment: *the authorized identified roles*].

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

Application Note 35: The role *terminal* is the default role for any terminal being recognized by the TOE as neither PACE terminal nor EAC2 terminal. The roles *CVCA*, *DV*, and *EAC2* terminal are recognized by analyzing the current Terminal Certificate, cf. [TR03110-2], (FIA_UAU.1/EAC2_Terminal). Specific types of EAC2 terminals are identified analogously. The TOE recognizes the electronic document holder by using a PACE terminal together with inputs PIN or PUK (FIA_UAU.1/PACE).
Here FMT_SMR.1.1 covers FMT_SMR.1.1/PACE in [PACEPP] and assigns additional roles (Role 5.-6.). BIS-PACE is renamed here to PACE terminal (Role 2). This extension does not conflict with the strict conformance to [PACEPP].

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

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

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions:
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles:
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/CVCA_INI
The TSF shall restrict the ability to write[55] the

1. initial CVCA Public Key ,
2. meta-data of the initial CVCA Certificate as required in [TR03110-2], resp. [TR03110-3],
3. initial Current Date,
4. [assignment: *list of TSF data*]

to [selection: *the manufacturer, the personalization agent*][56].

Application Note 36: The initial CVCA Public Key may be written by the *manufacturer* in the manufacturing phase or by the *personalization agent* in the issuing phase (cf. [TR03110-2]). The initial CVCA Public Keys and their updates later on are used to verify the CVCA Link-Certificates.

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

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/CVCA_UPD
The TSF shall restrict the ability to update[57] the

1. CVCA Public Key (PK_{CVCA}),
2. meta-data of the CVCA Certificate as required by [TR03110-2], resp. [TR03110-3][58],
3. [assignment: *list of TSF data*]

to the Country Verifying Certification Authority. [59]

Application Note 37: The CVCA updates its asymmetric key pair and distributes the public key and related meta-data by means of CVCA Link-Certificates. The TOE updates its internal trust-point, if a valid CVCA Link-Certificate (cf. FMT_MTD.3) is provided by the terminal (cf. [TR03110-3]).

55 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
56 [assignment: *the authorized identified roles*]
57 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
58 [assignment: *list of TSF data*]
59 [assignment: *the authorized identified roles*]

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

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/DATE
The TSF shall restrict the ability to modify [60] the current date[61] to

1. CVCA,
2. Document Verifier,
3. EAC2 terminal ([*assignment: list of EAC2 terminal types*]) possessing an Accurate Terminal Certificate according to [TR03110-3][62].
4. [assignment: *the authorized identified roles*]

Application Note 38: The authorized roles are identified in their certificates (cf. [TR03110-2]) and are authorized by validating the certificate chain up to the CVCA (cf. FMT_MTD.3). The authorized role of a terminal is part of the Certificate Holder Authorization in the card verifiable certificate that is provided by the terminal within Terminal Authentication 2 (cf. [TR03110-3]). Different types of EAC2 terminals may exist, cf. [TR03110-2]. They need to be defined, i.e. assigned in FMT_SMR.1 by the PP/ST writer.

FMT_MTD.1/PA Management of TSF data – Personalization Agent

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/PA
The TSF shall restrict the ability to write [63] the **card/chip security object(s) (SO_C) and** the document Security Object (SO_D)[64] to the Personalization Agent[65].

Application Note 39: Note that the card/chip security objects are mentioned here as well. These contain information, such as algorithm identifiers, only necessary for EAC2. All requirements formulated in [PACEPP] are thus met, and strict conformance is therefore not violated.

FMT_MTD.1/SK_PICC Management of TSF data – Chip Authentication and Restricted Identification Private Key(s)

Hierarchical to:
No other components.

60 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
61 [assignment: *list of TSF data*]
62 [assignment: *the authorized identified roles*]
63 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
64 [assignment: *list of TSF data*]
65 [assignment: *the authorized identified roles*]

Dependencies:
FMT_SMF.1 Specification of management functions:
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/SK_PICC
The TSF shall restrict the ability to [selection: *create, load*] [66] the Chip Authentication private key(s) (SK_{PICC}) and the Restricted Identification Private Key(s)[67] to the personalization agent[68].

Application Note 40: The component FMT_MTD.1/SK_{PICC} is refined by (i) selecting other operations and (ii) defining a selection for the operations 'create' and 'load' to be performed by the ST writer. The verb 'load' means here that the Chip Authentication private key(s) are securely generated outside the TOE and written into the TOE memory. The verb 'create' means here that the Chip Authentication private key(s) are generated by the TOE itself. In the latter case, the ST writer might include an appropriate instantiation of the component FCS_CKM.1 as an SFR for this key generation.

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

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/KEY_READ
The TSF shall restrict the ability to read[69] the

1. PACE passwords,
2. Personalization Agent Keys,
3. the Chip Authentication private key(s) (SK_{PICC})
4. the Restricted Identification private key(s)[70]
5. [assignment: *list of TSF data*]

to none[71].

Application Note 41: FMT_MTD.1/KEY_READ extends the SFR from [PACEPP] by additional assignments.

FMT_MTD.1/Initialize_PIN Management of TSF data – Initialize PIN

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

66 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
67 [assignment: *list of TSF data*]
68 [assignment: the authorized identified roles]
69 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
70 [assignment: *list of TSF data*]
71 [assignment: *the authorized identified roles*]

FMT_MTD.1.1/Initialize_PIN
The TSF shall restrict the ability to write[72] the initial PIN and PUK[73] to the personalization agent[74].

FMT_MTD.1/Resume_PIN Management of TSF data – Resuming PIN

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/Resume_PIN
The TSF shall restrict the ability to resume[75] the suspended PIN[76] to the electronic document holder[77].

Application Note 42: Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with the PIN. It must be implemented according to [TR03110-2], and is relevant for the status as required by FIA_AFL.1/Suspend_PIN. The electronic document holder is authenticated as required by FIA_UAU.1/PACE using the PIN as the shared password.

FMT_MTD.1/Change_PIN Management of TSF data – Changing PIN

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/Change_PIN
The TSF shall restrict the ability to change[78] the blocked PIN[79] to [assignment: *the authorised identified roles that match the list of PIN changing rules conformant to [TR03110-2]*][80]

FMT_MTD.1/Unblock_PIN Management of TSF data – Unblocking PIN

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

72 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
73 [assignment: *list of TSF data*]
74 [assignment: *the authorized identified roles*]
75 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
76 [assignment: *list of TSF data*]
77 [assignment: *the authorized identified roles*]
78 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
79 [assignment: *list of TSF data*]
80 [assignment: *the authorized identified roles*]

FMT_MTD.1.1/Unblock_PIN
The TSF shall restrict the ability to unblock[81] the blocked PIN[82] to

1. the electronic document holder (using the PUK for unblocking),
2. an EAC2 terminal of a type that has the terminal authorization level for PIN management.[83]

Application Note 43: The unblocking procedure must be implemented according to [TR03110-2], and is relevant for the status as required by FIA_AFL.1/Block_PIN. It can be triggered by either (i) the electronic document holder being authenticated as required by FIA_UAU.1/PACE using the PUK as the shared password or (ii) an EAC2 terminal (FIA_UAU.1/EAC2_Terminal) that proved a terminal authorization level being sufficient for PIN management (FDP_ACF.1/TRM).

FMT_MTD.1/Activate_PIN Management of TSF data – Activating/Deactivating PIN

Hierarchical to:
No other components.

Dependencies:
FMT_SMF.1 Specification of management functions
fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles
fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/Activate_PIN
The TSF shall restrict the ability to activate and deactivate[84] the PIN[85] to an EAC2 terminal of a type that has the terminal authorization level for PIN management[86].

Application Note 44: The activation/deactivation procedures must be implemented according to [TR03110-2]. They can be triggered by an EAC2 terminal (FIA_UAU.1/EAC2_Terminal) that proved a terminal authorization level sufficient for PIN management (FDP_ACF.1/TRM).

FMT_MTD.3 Secure TSF data

Hierarchical to:
No other components.

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

FMT_MTD.3.1
The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control SFP[87].

Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [TR03110-3].

Application Note 45: Terminal Authentication is used as required by (i) FIA_UAU.1/EAC2_Terminal and FIA_UAU.5. The terminal authorization level derived from the CVCA Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access control required by FDP_ACF.1/TRM.

In addition, this PP contains all remaining SFRs of the claimed PP [PACEPP].

81 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
82 [assignment: *list of TSF data*]
83 [assignment: *the authorized identified roles*]
84 [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
85 [assignment: *list of TSF data*]
86 [assignment: *the authorized identified roles*]
87 [assignment: list of TSF data]

- **FMT_LIM.1**
- **FMT_LIM.2**
- **FMT_MTD.1/INI_ENA**
- **FMT_MTD.1/INI_DIS**

6.1.7 Class FPT

The TOE shall prevent inherent and forced illicit information leakage for user data and TSF-data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. W.r.t. forced leakage, the requirements have to be considered in combination with the security functional requirements *Failure with preservation of secure state (FPT_FLS.1)* and *TSF testing (FPT_TST.1)* on the one hand, and *Resistance to physical attack* (FPT_PHP.3) on the other hand. The SFRs *Limited capabilities* (FMT_LIM.1), *Limited availability* (FMT_LIM.2) and *Resistance to physical attack* (FPT_PHP.3), together with the design measures to be described within the SAR *Security architecture description* (ADV_ARC.1), prevent bypassing, deactivation and manipulation of security features, or misuse of the TOE security functionality.

FPT_EMS.1 TOE Emanation

Hierarchical to:
No other components.

Dependencies:
No dependencies.

FPT_EMS.1.1
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}),**
2. the ephemeral private key ephem-SK_{PICC}-PACE[88],
3. the Chip Authentication private keys (SK_{PICC})
4. the PIN, PUK,
5. [assignment: *list of types of TSF data*]

and

6. the Restricted Identification private key(s) SK_{ID}[89],
7. [assignment: *list of types of user data*].

FPT_EMS.1.2
The TSF shall ensure any users[90] are unable to use the following interface electronic document's contactless/contact-based interface and circuit contacts[91] to gain access to

1. **the** session keys (PACE-K_{MAC}, PACE-K_{Enc}), **(CA-K_{MAC}, CA-K_{Enc}),**
2. the ephemeral private key ephem-SK_{PICC}-PACE1,
3. the Chip Authentication private key(s) (SK_{PICC}),
4. the PIN, PUK,

88 [assignment: *list of types of TSF data*]
89 [assignment: *list of types of user data*]
90 [assignment: *type of users*]
91 [assignment: *type of connection*]

5. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc})[92]
6. [assignment: *list of types of TSF data*]

and

7. the Restricted Identification private key(s) SK_{ID},[93]
8. [assignment: *list of types of user data*].

Application Note 46: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power consumption, timing of signals, and electromagnetic radiation due to internal operations or data transmissions.
Note that while the security functionality described in FPT_EMS.1 should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development.
Note that in the above SFR, all items in FPT_EMS.1.2 from 3. upwards are additional assignments. The first item is slightly refined to include CA-key(s)

In addition, this PP contains all remaining SFRs of the claimed PP [PACEPP].

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

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are chosen 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 security functional requirements coverage. It also gives an evidence for sufficiency and necessity of the chosen SFRs. Security objectives and SFRs that are taken verbatim from [PACEPP] are printed in *cursive* style.

92 [assignment: *list of types of TSF data*]
93 [assignment: *list of types of user data*]

	OT.Identification	OT.AC_Pers_EAC2	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse_Func*	*OT.Prot_Inf_Leak*	*OT.Prot_Phys_Tamper*	*OT.Prot_Malfunction*	OT.CA2	OT.RI_EAC2	OT.Sens_Data_EAC2
FCS_CKM.1/DH_PACE			x	x	x						x		x
FCS_COP.1/SHA			x	x	x						x		x
FCS_COP.1/SIG_VER			x	x	x								x
FCS_COP.1/PACE_ENC					x								x
FCS_COP.1/PACE_MAC			x	x							x		
FCS_CKM.4			x	x	x								x
FCS_RND.1			x	x	x						x		x
FIA_AFL.1/Suspend_PIN		x	x	x	x								x
FIA_AFL.1/Block_PIN		x	x	x	x	x							x
FIA_API.1/CA			x	x	x						x		x
FIA_API.1/RI												x	
FIA_UID.1/PACE			x	x	x								x
FIA_UID.1/EAC2_Terminal		x	x	x	x								x
FIA_UAU.1/PACE			x	x	x								x
FIA_UAU.1/EAC2_Terminal		x	x	x	x								x
FIA_UAU.4/PACE			x	x	x								x
FIA_UAU.5/PACE			x	x	x							x	x
FIA_UAU.6/CA			x	x	x								x
FIA_AFL.1/PACE						x							
FIA_UAU.6/PACE			x	x	x								x
FDP_ACF.1/TRM		x	x		x								x
FDP_RIP.1		x	x	x	x						x		x
FDP_ACC.1/TRM		x	x		x								x
FDP_UCT.1/TRM			x		x								x
FDP_UIT.1/TRM			x		x								x
FTP_ITC.1/PACE			x	x	x	x							x
FTP_ITC.1/CA2			x	x	x	x							x
FAU_SAS.1	x	x											
FMT_SMF.1	x	x	x	x	x								x
FMT_SMR.1/PACE	x	x	x	x	x								x
FMT_MTD.1/CVCA_INI			x	x	x								x
FMT_MTD.1/CVCA_UPD			x	x	x								x
FMT_MTD.1/DATE			x	x	x								x
FMT_MTD.1/PA		x	x	x	x						x		x
FMT_MTD.1/SK_PICC			x	x	x						x		x
FMT_MTD.1/KEY_READ		x	x	x	x						x		x
FMT_MTD.1/Initialize_PIN		x	x	x	x								x
FMT_MTD.1/Resume_PIN		x	x	x	x								x
FMT_MTD.1/Change_PIN		x	x	x	x								x
FMT_MTD.1/Unblock_PIN		x	x	x	x								x
FMT_MTD.1/Activate_PIN		x	x	x	x								x
FMT_MTD.3			x	x	x								x
FMT_LIM.1							x						
FMT_LIM.2							x						
FMT_MTD.1/INI_ENA	x	x											
FMT_MTD.1/INI_DIS	x	x											
FPT_EMS.1								x					

	OT.Identification	*OT.AC_Pers_EAC2*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse_Func*	*OT.Prot_Inf_Leak*	*OT.Prot_Phys_Tamper*	*OT.Prot_Malfunction*	OT.CA2	OT.RI_EAC2	OT.Sens_Data_EAC2
FPT_FLS.1								x		x			
FPT_TST.1								x		x			
FPT_PHP.3			x					x	x				

Table 3: Coverage of Security Objectives for the TOE by SFRs

1115 To achieve the security objectives of the TOE, the security functional requirements must be suitable. A detailed justification for this suitability is given below.

OT.Identification

The security objective **OT.Identification** addresses the storage of initialization and pre-personalization data in its non-volatile memory. This data includes the IC identification data that uniquely identify the TOE's chip. This is ensured by **FAU_SAS.1**. The SFR **FMT_MTD.1/INI_ENA** allows only the manufacturer to write
1120 initialization and pre-personalization data (including the personalization agent key). The **SFR FMT_MTD.1/INI_DIS** requires the personalization agent to disable access to initialization and pre-personalization data in the life cycle phase operational use. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the related functions and roles.

OT.AC_Pers_EAC2

The security objective **OT.AC_Pers_EAC2** ensures that only the personalization agent can write user- and
1125 TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM** requiring, amongst other, an appropriate authorization level of an EAC2 terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs **FIA_UID.1/EAC2_Terminal** and **FIA_UAU.1/EAC2_Terminal**. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the related functions and roles. Since only an EAC2 terminal can reach the
1130 necessary authorization level, using and managing the PIN (the related SFRs are **FIA_AFL.1/Suspend_PIN**, **FIA_AFL.1/Block_PIN**, **FMT_MTD.1/Resume_PIN**, **FMT_MTD.1/Change_PIN**, **FMT_MTD.1/Unblock_PIN**, and **FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN**) also support the achievement of this objective. **FDP_RIP.1** requires erasing the temporal values PIN and PUK. The justification for the SFRs **FAU_SAS.1**, **FMT_MTD.1/INI_ENA** and **FMT_MTD.1/INI_DIS** arises from the justification for OT.Identification above
1135 with respect to the pre-personalization data. **FMT_MTD.1/PA** covers the related property of **OT.AC_Pers_EAC2** (writing/updating SO_C and SO_D and, in generally, personalization data). Updating such data can only be done by the personalization agent prior to the operational phase. Thus such data cannot be changed after the personalization of the document, as required by **OT.AC_Pers_EAC2**. Finally, **FMT_MTD.1/KEY_READ** ensures that cryptographic keys for EAC2 can not be read by users.

OT.Data_Integrity

1140 The security objective **OT.Data_Integrity** ensures that the TOE always ensures integrity of stored user- and TSF-Data and, after Terminal- and Chip Authentication 2, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by **FPT_PHP.3**.
Unauthorized modifying of the stored data is addressed by **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM**. Enforcement of the two previous in a protected manner is ensured by **FDP_UCT.1/TRM** and **FDP_UIT.1/TRM**.
1145 A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs **FIA_UID.1/EAC2_Terminal**, **FIA_UAU.1/EAC2_Terminal**, supported by **FCS_COP.1/SIG_VER**. The TA2 protocol uses the result of PACE authentication (**FIA_UID.1/PACE**, **FIA_UAU.1/PACE**) being, in turn, supported by **FCS_CKM.1/DH_PACE**. Since PACE can use the PIN as the shared secret, using and management of PIN

(**FIA_AFL.1/Suspend_PIN**, **FIA_AFL.1/Block_PIN**, **FMT_MTD.1/Resume_PIN**, **FMT_MTD.1/Change_PIN**, **FMT_MTD.1/Unblock_PIN**, **FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PIN)** also support achievement of this objective. **FDP_RIP.1** requires erasing the temporal values of PIN, PUK.
FIA_UAU.4/PACE, **FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the used protocols.
To allow for a verification of the certificate chain as required in **FMT_MTD.3**, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD** and **FMT_MTD.1/DATE**.
Unauthorized modifying of the exchanged data is addressed by **FTP_ITC.1/CA2** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_MAC**. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. **FIA_API.1/CA** using **FCS_CKM.1/DH_PACE** possessing the special properties **FIA_UAU.5/PACE** and **FIA_UAU.6/CA**. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using **FIA_UID.1/PACE**, **FIA_UAU.1/PACE** and **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, **FIA_UAU.6/PACE**.

CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). **FMT_MTD.1/SK_PICC** governs creating/loading SK_{PICC}, and **FMT_MTD.1/KEY_READ** requires SK_{PICC} to be unreadable by users; thus its value remains confidential. **FDP_RIP.1** requires erasing the values of SK_{PICC} and session keys (here: for K_{MAC}).
FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified only by the personalization agent. Hence, is to considered as trustworthy.
The SFRs **FCS_COP.1/SHA** and **FCS_RND.1** represent general support required for cryptographic operations.
The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support related functions and roles.

OT.Data_Authenticity

The security objective **OT.Data_Authenticity** ensures the authenticity of user- and TSF-Data (after Terminal- and the Chip Authentication 2) by enabling its verification on both the terminal-side and by an active verification by the TOE itself.
This objective is mainly achieved by **FTP_ITC.1/CA2** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_MAC**. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. **FIA_API.1/CA** using **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, and **FIA_UAU.6/CA**. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using **FIA_UID.1/PACE**, **FIA_UAU.1/PACE** and **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, **FIA_UAU.6/PACE**.

CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). **FMT_MTD.1/SK_PICC** governs creating/loading SK_{PICC}, **FMT_MTD.1/KEY_READ** requires to make this key unreadable by users. Hence its value remains confidential. **FDP_RIP.1** requires to erase the values of SK_{PICC} and session keys, here for K_{MAC}.

FMT_MTD.1/PA requires that the SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy.
A prerequisite for successful CA2 is an accomplished TA2 as required by **FIA_UID.1/EAC2_Terminal**, **FIA_UAU.1/EAC2_Terminal**, supported by **FCS_COP.1/SIG_VER**. The TA2 protocol uses the result of the PACE authentication (**FIA_UID.1/PACE**, **FIA_UAU.1/PACE**) being, in turn, supported by **FCS_CKM.1/DH_PACE**. Since PACE can use the PIN as the shared secret, the use and management of the PIN (**FIA_AFL.1/Suspend_PIN**, **FIA_AFL.1/Block_PIN**, **FMT_MTD.1/Resume_PIN**, **MT_MTD.1/Initialize_PIN, FMT_MTD.1/Change_PIN**, **FMT_MTD.1/Unblock_PIN**, **FMT_MTD.1/Activate_PIN**) also support achieving this objective. **FDP_RIP.1** requires to erase the temporal values of the PIN and PUK.
FIA_UAU.4/PACE, **FIA_UAU.5/PACE, FIA_UAU.6/CA** and **FCS_CKM.4** represent some specific required properties of the used protocols.
To allow for a verification of the certificate chain as required in **FMT_MTD.3**, the CVCA's public key and cer-

tificate, as well as the current date, are written or updated by authorized identified roles as required by **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD** and **FMT_MTD.1/DATE**.
The SFRs **FCS_COP.1/SHA** and **FCS_RND.1** represent the general required support for cryptographic operations.
The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the related functions and roles.

OT.Data_Confidentiality

The security objective **OT.Data_Confidentiality** ensures that the TOE always ensures confidentiality of the user- and TSF-Data stored and, after Terminal- and Chip Authentication 2, of their exchange.
This objective for the data stored is mainly achieved by **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM**. Enforcement of the two previous in a protected manner is ensured by **FDP_UCT.1/TRM** and **FDP_UIT.1/TRM**. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs **FIA_UID.1/EAC2_Terminal**, **FIA_UAU.1/EAC2_Terminal**, supported by **FCS_COP.1/SIG_VER**. The TA2 protocol uses the result of the PACE authentication (**FIA_UID.1/PACE**, **FIA_UAU.1/PACE,** confidentiality of the PACE passwords is ensured by **FMT_MTD.1/KEY_READ**) being, in turn, supported by **FCS_CKM.1/DH_PACE**. Since PACE can use the PIN as the shared secret, the use and management of the PIN (**FIA_AFL.1/Suspend_PIN**, **FIA_AFL.1/Block_PIN**, **FMT_MTD.1/Resume_PIN**, **FMT_MTD.1/Unblock_PIN**, **FMT_MTD.1/Change_PIN**, **MT_MTD.1/Initialize_PIN,** **FMT_MTD.1/Activate_PIN**) also support to achieve this objective. **FDP_RIP.1** requires erasing the temporal values of the PIN and PUK.
FIA_UAU.4/PACE, **FIA_UAU.5/PACE, FIA_UAU.6/PACE** and **FCS_CKM.4** represent some specific properties of the used protocols.
To allow for a verification of the certificate chain as required in **FMT_MTD.3**, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD** and **FMT_MTD.1/DATE**.
This objective for the data exchanged is mainly achieved by **FTP_ITC.1/CA2** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_ENC**. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. **FIA_API.1/CA** using **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, and **FIA_UAU.6/CA**. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using **FIA_UID.1/PACE, FIA_UAU.1/PACE** and **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE, FIA_UAU.6/PACE**.

CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). **FMT_MTD.1/SK_PICC** governs creating/loading SK_{PICC}, **FMT_MTD.1/KEY_READ** requires making this key unreadable by users. Thus its value remains confidential. **FDP_RIP.1** requires erasing the values of SK_{PICC} and session keys, here for K_{ENC}.
FMT_MTD.1/PA requires that only the the personalization agent is allowed to modify the SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication.
The SFRs **FCS_COP.1/SHA** and **FCS_RND.1** represent the general required support for cryptographic operations.
The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the related functions and roles.

OT.Sens_Data_EAC2

The security objective of **OT.Sens_Data_EAC2** aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (**FDP_UCT.1/TRM** and **FDP_UIT.1/TRM**) the access control SFPs **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM**.
A specific authorization level is achieved by terminal identification/authentication as required by the SFRs **FIA_UID.1/EAC2_Terminal**, **FIA_UAU.1/EAC2_Terminal**, supported by **FCS_COP.1/SIG_VER**. The TA2 protocol uses the result of the PACE authentication (**FIA_UID.1/PACE**, **FIA_UAU.1/PACE,** confidentiality of the PACE passwords is ensured by **FMT_MTD.1/KEY_READ**) being, in turn, supported by **FCS_CKM.1/DH_PACE**. Since PACE can use the PIN as the shared secret, the use and management of the PIN (**FIA_AFL.1/Suspend_PIN**, **FIA_AFL.1/Block_PIN**, **FMT_MTD.1/Resume_PIN**, **FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PIN**, **FMT_MTD.1/Change_PIN**, **FMT_MTD.1/Activate_PIN**) also support to achieve this objective. **FDP_RIP.1** requires erasing the temporal values of the PIN

and PUK.
FIA_UAU.4/PACE, **FIA_UAU.5/PACE, FIA_UAU.6/PACE** and **FCS_CKM.4** represent some specific properties
1250 of the used protocols.
To allow for a verification of the certificate chain as required in **FMT_MTD.3**, the CVCA's public key and certificate as well as the current date are written or updated by authorized identified role as required by **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD** and **FMT_MTD.1/DATE**.
This objective for the data exchanged is mainly achieved by **FTP_ITC.1/CA2** and **FTP_ITC.1/PACE** using
1255 **FCS_COP.1/PACE_ENC**. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. **FIA_API.1/CA** using **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, and **FIA_UAU.6/CA**. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using **FIA_UID.1/PACE, FIA_UAU.1/PACE** and **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE, FIA_UAU.6/PACE**.
1260 CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). **FMT_MTD.1/SK_PICC** governs creating/loading SK_{PICC}, **FMT_MTD.1/KEY_READ** requires making this key unreadable by users. Thus its value remains confidential. **FDP_RIP.1** requires erasing the values of SK_{PICC} and session keys, here for K_{ENC}.
FMT_MTD.1/PA requires that only the the personalization agent is allowed to modify the SO_C (containing
1265 amongst other, the signature of PK_{PICC}) used for Passive Authentication.
The SFRs **FCS_COP.1/SHA** and **FCS_RND.1** represent the general required support for cryptographic operations.
The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the related functions and roles.

OT.Prot_Abuse_Func

The rationale is analogous to [PACEPP].

OT.Prot_Phys_Temper

1270 The rationale is analogous to [PACEPP].

OT.Prot_Malfunction

The rationale is analogous to [PACEPP].

OT.Tracing

The security objective **OT.Tracing** ensures that the TOE prevents gathering TOE tracing data by means of unambiguously identifying the electronic document remotely through establishing or listening to communication via the contactless/contact-based interface of the TOE without a priori knowledge of the correct
1275 values of shared passwords (CAN, MRZ, PIN, PUK).
This objective is achieved as follows:

1. While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data) by **FIA_AFL.1/PACE,**
2. while establishing PACE communication using the PIN (blocking authentication data) by
1280 **FIA_AFL.1/Block_PIN,**
3. for listening to PACE communication and for establishing CA2 communication (which is of importance for the current PP, if Chip Security Object and PK_{PICC} are card-individual) by **FTP_ITC.1/PACE**,
4. and for listening to CA2 communication (readable and writable user data: document details data, biographic data, biometric reference data) by **FTP_ITC.1/CA2**.

OT.CA2

1285 The security objective **OT.CA2** aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by **FIA_API.1/CA** using **FCS_CKM.1/DH_PACE**. CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). **FMT_MTD.1/SK_PICC** governs creating/loading

SK_{PICC}, whereas **FMT_MTD.1/KEY_READ** requires making this key unreadable by users. Hence, its value remains confidential. **FDP_RIP.1** requires erasing the values of SK_{PICC} and the session keys, here for CMAC.
The authentication token T_{PICC} is calculated using **FCS_COP.1/PACE_MAC**. The SFRs **FCS_COP.1/SHA** and **FCS_RND.1** represent the general required support for cryptographic operations.
FMT_MTD.1/PA requires that the SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy.

OT.Prot_Inf_Leak

The security objective **OT.Prot_Inf_Leak** aims at protection against disclosure of confidential user- or/and TSF-data stored on or processed by the TOE.
This objective is achieved by

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

OT.RI_EAC2

The security objective **OT.RI_EAC2** aims at providing a way to pseudnoymously identify an electronic document holder without granting a terminal read access to sensitive user data. This objective is covered by **FIA_API.1/RI** which requires the TOE to implement the Restricted Identification protocol as specified in [TR03110-2]. It is supported by **FIA_UAU.5/PACE**, which identifies some specific properties of the protocol, here in particular that RI should be (optionally) performed after successful TA2 and CA2.
The rationale related to the security objectives taken over from [PACEPP] are exactly the same as in the given reference.

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 component definitions 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. 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:

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.

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 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 document and displayed by it using e.g. ePaper, an OLED or similar technologies), cf. [TR03110-2] and [ICAO9303].

Card Security Object (SO_C)

An RFC3369 CMS signed data structure signed by the Document Signer (DS). It is stored in the electronic document (EF.CardSecurity or resp. EF.ChipSecurity,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).

Chip Authentication Private Key

Private key used within the Chip Authentication protocol, cf. [TR03110-2]

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 EAC2 terminals and creates document verifier 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, see [TR03110-3].

Document Security Object (SO_D)

A RFC3369 CMS signed data structure, signed by the Document Signer (DS). 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 (DS)

An organization enforcing the policy of the CSCA and signing the electronic document security object stored on the eID-Card 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 EAC2 terminals, see [TR03110-3].

Extended Access Control 2 (EAC2)
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 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 an optical readable part. An 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).

Integrated circuit (IC)
Electronic component(s) designed to perform processing and/or memory functions. The electronic document's chip is an integrated circuit.

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].

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

PACE Session Key
Session key constructed during execution of the PACE protocol, cf. [TR03110-2]

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 ([TR03110-2]).

Restricted Identification Private Key
Private key used within the Restricted Identity protocol, cf. [TR03110-2]

EAC2 Terminal
An EAC2 terminal refers to a technical device possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective CVCA.

Secure Messaging
Secure messaging using encryption and message authentication code according to [ISO7816-4]. Secure messaging according to [ISO7816-4] employs the encrypt-then-authenticate approach to build an encryption scheme.

Terminal Authorization Level
Intersection of the Certificate Holder Authorizations defined by the terminal certificate, the document verifier certificate and Country Verifying Certification Authority which shall be all valid for the current date. The authorization level can additionally be restricted at a terminal by the electronic document holder with the help of the CHAT.

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
1500	PCD	Proximity Coupling Device
	PICC	Proximity Integrated Circuit Chip
	PIN	Personal Identification Number
	PP	Protection Profile
	PUK	PIN Unblock Key
1505	RF	Radio Frequency
	SAR	Security assurance requirements
	SFR	Security functional requirement
	SO_C	Chip/Card Security Object
	TA	Terminal Authentication
1510	TOE	Target of Evaluation
	TSF	TOE security functionality
	TSP	TOE Security Policy (defined by the current document)

References

CC1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2012-09-001, September 2012
CC2	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, September 2012
CC3	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, September 2012
CC4	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004 , September 2012
FIPS180-4	National Institute of Standards and Technology: FIPS PUB 180-4: Secure hash standard, March 2012.
ICAO-SAC	ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.01, 11. November 2010.
ICAO9303	ICAO: ICAO Doc 9303 - Machine Readable Travel Documents, Part 1, Volume 2, 6th edition, 2006
ISO14443	ISO/IEC: ISO/IEC 14443:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008
ISO7816-2	ISO/IEC: ISO/IEC 7816-2:2007: Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts, 2007
ISO7816-4	ISO/IEC: ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange, 2013
PACEPP	Bundesamt für Sicherheit in der Informationstechnik: Common Criteria Protection Profile - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA01, Version 1.01, 22.07.2014
PKCS3	RSA Laboratories: PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4,Revised November 1, 1993
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), Version 2.10, 20. March 2012
TR03110-3	BSI: TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents. Part 3 - Common Specifications, Version 2.10, 20. March 2012
TR03111	BSI: TR 03111: Elliptic Curve Cryptography, Version 2.0, 28. June 2012.
TR03116-2	BSI: TR 03116-2: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, 2. February 2015