Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Electronic Identity Card (ID_Card PP)

BSI-CC-PP-0061

Approved by the
Federal Ministry of Interior

Version 1.03, 15th December 2009

Foreword

This Protection Profile 'Electronic Identity Card (ID_Card PP)' is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 3.1 [1], [2], [3], Revision 3.

Correspondence and comments to this Protection Profile should be referred to:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn, Germany

Phone: **+49 228 99 9582-0**
Fax: **+49 228 99 9582-400**

Email: **bsi@bsi.bund.de**

Contents

1 PP Introduction 5
1.1 PP reference 5
1.2 TOE Overview 5
1.2.1 TOE definition and operational usage 5
1.2.2 TOE major security features for operational use 7
1.2.3 TOE type 7
1.2.4 Non-TOE hardware/software/firmware 7
2 Conformance Claims 11
2.1 CC Conformance Claim 11
2.2 PP Claim 11
2.3 Package Claim 12
2.4 Conformance Claim Rationale 12
2.4.1 'Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation' 12
2.5 Conformance statement 13
3 Security Problem Definition 14
3.1 Introduction 14
3.2 Threats 22
3.3 Organisational Security Policies 25
3.4 Assumptions 29
4 Security Objectives 30
4.1 Security Objectives for the TOE 30
4.2 Security Objectives for Operational Environment 34
4.3 Security Objective Rationale 39
5 Extended Components Definition 42
5.1 Definition of the Family FAU_SAS 42
5.2 Definition of the Family FCS_RND 42
5.3 Definition of the Family FIA_API 43
5.4 Definition of the Family FMT_LIM 44
5.5 Definition of the Family FPT_EMSEC 46
6 Security Requirements 48
6.1 Security Functional Requirements for the TOE 48
6.1.1 Overview 48
6.1.2 Class FCS Cryptographic Support 53
6.1.3 Class FIA Identification and Authentication 59

6.1.4 Class FDP User Data Protection 68
6.1.5 Class FTP Trusted Path/Channels 72
6.1.6 Class FAU Security Audit 73
6.1.7 Class FMT Security Management 74
6.1.8 Class FPT Protection of the Security Functions 84
6.2 Security Assurance Requirements for the TOE 87
6.3 Security Requirements Rationale 88
6.3.1 Security Functional Requirements Rationale 88
6.3.2 Rationale for SFR's Dependencies 93
6.3.3 Security Assurance Requirements Rationale 93
6.3.4 Security Requirements – Internal Consistency 94
7 Glossary and Acronyms 96
8 Bibliography 107

List of Tables

Table 1: ID_Card applications vs. terminal types 10
Table 2: Primary assets 15
Table 3: Secondary assets 16
Table 4: Subjects and external entities 21
Table 5: Threats taken over from [7] 25
Table 6: OSPs taken over from [7] 29
Table 7: Assumptions taken over from [7] 29
Table 8: TOE objectives taken over from [7] 33
Table 9: TOE's environment objectives taken over from [7] 39
Table 10: Security Objective Rationale 40
Table 11: Security functional groups vs. SFRs 51
Table 12: Keys and Certificates 53
Table 13: Overview of authentication SFRs 59
Table 14: Coverage of Security Objectives for the TOE by SFR 89
Table 15: SAR Dependencies 94

1 PP Introduction

1 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

2 Title:	Protection Profile 'Electronic Identity Card (ID_Card PP)'
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
Editor(s):	Dr. Igor Furgel T-Systems GEI GmbH, SC Security Analysis & Testing
CC Version:	3.1 (Revision 3)
Assurance Level:	Minimum assurance level for this PP is EAL4 augmented.
General Status:	Final
Version Number:	1.03 as of 15th December 2009
Registration:	BSI-CC-PP-0061
Keywords:	Electronic Identity Card, ID_Card, ePassport, eID, eSign, MRTD, PACE, EAC

1.2 TOE Overview

1.2.1 TOE definition and operational usage

3 The Target of Evaluation (TOE) addressed by the current protection profile is electronic Identity Card (ID_Card) representing a contactless smart card programmed according to BSI TR-03110, version 2.02 [11]. This smart card provides the following applications:

– the *ePassport*[1] containing the related user data[2] (incl. biometric) as well as data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD);
– the *eID*[3] including the related user data[4] and data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application;
– the *eSign*[5] containing data needed for generating advanced or qualified electronic (concretely: digital) signatures on behalf of the ID_Card holder as well as for authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified digital signature of the ID_Card holder is required. The eSign application is optional: it

[1] as specified in [11], sec. 3.1.1; see also [8], [9].

[2] according to [11], sec. 1.1 and 3.1.1; see also chap. 7 below for definitions

[3] as specified in [11], sec. 3.1.2

[4] according to [11], sec. 3.1.2

[5] as specified in [11], sec. 3.1.3

means that it can optionally be activated on the ID_Card by a Certification Service Provider (or on his behalf).

4 For the *ePassport* application, the ID_Card holder can control access to his user data by conscious presenting his ID_Card to authorities[6].

5 For the *eID* application, the ID_Card holder can control access to his user data by inputting his secret PIN (eID-PIN) or by conscious presenting his ID_Card to authorities[7].

6 For the *eSign* application, the ID_Card holder can control access to the digital signature functionality by conscious presenting his ID_Card to a service provider and inputting his secret PIN for this application: eSign-PIN[8].

7 *Application note 1:* In principle, it might technically be possible to grant access to the digital signature functionality by inputting CAN only (see [11], sec. 3.3); however, this technical option shall not be allowed by the security policy defined for the eSign application (see the related conformance claim in sec. 2.2 below) due to the fact that solely the Signatory (here: the ID_Card holder) shall be able to generate a digital signature on his own behalf.

8 *Application note 2:* Using a secret PIN by the PIN's owner represents a manifestation of his declaration of intent bound to this secret PIN. In order to reflect this fact, the eID and the eSign applications shall organisationally get different values of the respective secret PINs (eID-PIN and eSign-PIN). It is especially important, if qualified electronic signatures shall be generated by the eSign application.

9 The ID_Card is integrated into a plastic, optically readable part of the Identity Card, which – as the final product – shall supersede the existing, merely optically readable Identity Cards. The plastic, optically readable cover of the Identity Card, where the electronic Identity Card is embedded in, is not part of the TOE. The tying-up of the electronic Identity Card to the plastic Identity Card is achieved by physical and organisational security measures being out of scope of the current PP.

10 The TOE shall comprise at least

i) the circuitry of the contactless chip incl. all IC dedicated software[9] being active in the operational phase of the TOE (the integrated circuit, IC),

ii) the IC Embedded Software (operating system)[10],

iii) the ePassport, the eID and, optionally[11], the eSign applications and

iv) the associated guidance documentation.

11 *Application note 3:* Since contactless interface parts (e.g. antenna) may have impact on specific aspects of vulnerability assessment and, thus, be security relevant, these parts might be

[6] CAN or MRZ user authentication, see [11], sec. 3.3

[7] eID-PIN or CAN user authentication, see [11], sec. 3.3

[8] CAN and eSign-PIN user authentication, see [11], sec. 3.3

[9] usually preloaded (and often security certified) by the Chip Manufacturer

[10] usually – together with IC – completely implementing executable functions

[11] it means activated or not activated on the ID_Card

considered as part of the TOE. The decision upon this is up to the certification body in charge by defining the evaluation methodology for the assessment of the contactless interface.

1.2.2 TOE major security features for operational use

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

– Only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the ID_Card under control of the ID_Card holder,
– Verifying authenticity and integrity as well as securing confidentiality of user data[12] in the communication channel between the TOE and the service provider connected[13],
– Creation of digital signatures, if the eSign application is operational,
– Averting of inconspicuous tracing of the ID_Card,
– Self-protection of the TOE security functionality and the data stored inside.

1.2.3 TOE type

13 The TOE type is contactless smart card with the ePassport, the eID and the eSign applications named as a whole 'electronic Identity Card (ID_Card)'.

14 The typical life phases for the current TOE type are development[14], manufacturing[15], card issuing[16] and, finally, operational use. Operational use of the TOE is explicitly in focus of the current PP. Some single properties of the manufacturing and the card issuing life phases being significant for the security of the TOE in its operational phase are also considered by the current PP. A security evaluation/certification being conform with this PP will have to involve all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 2.3 'Package Claim' below).

1.2.4 Non-TOE hardware/software/firmware

15 In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless communication according to [20].

16 From the logical point of view, the TOE shall be able to distinguish between the following terminal types, which, hence, shall be available (see [11], sec. 3.2):

– *Inspection system*: an official terminal that is always operated by a governmental organisation

[12] please note that user data might also be imported from outside of the TOE, e.g. data to be signed by the eSign application

[13] a service provider can technically be represented by a local RF-terminal as the end point of secure communication in the sense of this PP (local authentication) or by a remote terminal as the end point of secure communication in the sense of this PP (online authentication)

[14] IC itself and IC embedded software

[15] IC manufacturing and smart card manufacturing including installation of a native card operating system

[16] including installation of the smart card applications and their electronic personalisation (i.e. tying the application data up to the ID_Card holder)

(i.e. an Official Domestic or Foreign Document Verifier),
– *Authentication terminal*: a terminal that may be operated by a governmental organisation (Official Domestic Document Verifier) or by any other organisation (Non-Official / Foreign Document Verifier), and
– *Signature terminal*: a terminal used by ID_Card holder for generation of digital signatures.

17 The TOE shall require terminal of each type to authenticate itself before access according to effective terminal authorisation is granted. To authenticate a terminal either as an inspection system or authentication terminal or signature terminal, General Authentication Procedure[17] must be used.

18 *Application note 4:* The specification [11], sec. 3.2 knows only one type of inspection systems, namely according to the result of the terminal authentication in the context of the General Authentication Procedure. It means that the Inspection System in the context of [11] (and of the current PP) is commensurate with the Extended Inspection System (EIS) as defined in [6][18].
Some developers might decide to implement their products being downwardly compatible with ICAO-terminals[19], so that they also support Basic Access Control (BAC), see [11], sec. 1.1, 3.1.1 and Appendix G. A terminal authenticated by BAC[20] (see [11], Appendix H) also represents a kind of inspection system, which we also call here Basic Inspection System (BIS) as already done in [6].
<u>However, any product supporting BAC will not be conformant to the current PP.</u>

19 *Application note 5:* A [11]-compliant terminal shall always start a communication session using PACE. If successful, it shall then proceed with terminal- and chip-authentications as required by GAP in [11]. Terminal will be authorised (depending on its certificate) as the Inspection System in the sense of [11] (equivalent to EIS in [6]).
If the trial with PACE failed, the [11]-compliant terminal may try to establish a communication session using BAC. If successful, the terminal can be authorised as BIS (equivalent to BIS in [6]), if the concrete product supports BAC.
A non-compliant terminal may directly start a communication session using BAC. If successful, the terminal can be authorised as BIS (equivalent to BIS in [6]), if the concrete product supports BAC.
There may also be a technical opportunity for using different orders of chip and terminal authentication protocols by a [11]-compliant terminal. <u>The security policy of the current PP covers only the sequence 'PACE' -> 'terminal authentication' -> 'passive authentication' -> 'chip authentication' as depicted in Fig. 3.1, sec. 3.1.1 of [11], the branch rightmost (General Authentication Procedure, sec. 3.4 of [11])</u>.
<u>Please note that the current TOE does not support BAC.</u>

20 *Application note 6:* After Terminal Authentication. Passive Authentication and Chip Authentication have successfully been performed, the authenticated terminal can request for a sector-specific chip-identifier (Restricted Identification, see sec. 2.1.5, 3.2, 4.5 of [11]). Restricted Identification aims providing a temporary ID_Card identifier being specific for a terminal sector (pseudo-anonymisation) and supporting revocation features (sec. 3.2, 4.1.2 of [11]). The security status of ID_Card is not affected by Restricted Identification.

---

[17] i.e. PACE, terminal authentication, passive authentication and chip authentication according to [11], sec. 4.2, 4.3 and 4.4

[18] please note that an Extended Inspection System also covers the General Inspection Systems (GIS) in the sense of [6]

[19] so called non-compliant inspection systems not supporting PACE, see [11], Appendix G

[20] i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the Identity Card

21 *Application note 7:* Concerning terminals for the eSign application, the parallels with the terminals as defined in [7] are as follows: the Authentication Terminal in the context of [11] (and of the current PP) is CGA[21] in [7]; the Signature Terminal in the context of [11] represents a combination of SCA[22] and HID[23] in [7].

22 The authorisation level of an authenticated terminal shall be determined by the effective terminal authorisation calculated from the certificate chain presented by this terminal to the TOE[24]. All necessary certificates of the related public key infrastructure – Country Verifying Certification Authority (CVCA) Link Certificates, Document Verifiers Certificates and Terminal Certificates – shall be available in a card verifiable format as specified in [11], Appendix C.1; see also [11], sec. 2.2.3.

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

	Inspection System (official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
ePassport	Operations: reading all data groups (incl. biometrical) User interaction: CAN or MRZ for PACE In this context, the current terminal is equivalent to EIS in	-	-

[21] Certification Generation Application

[22] Signature Creation Application

[23] Human Interface Device

[24] It is based on Certificate Holder Authorization Template (CHAT), see [11], C.1.5. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ID_Card holder's restricting input at the terminal. This final CHAT reflects the *effective authorisation level*, see [11], C.4.2 and is then sent to the TOE by the command 'MSE:Set AT' within the Terminal Authentication (B.3 und B.11.1 of [11]).

	Inspection System (official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
	[6]		
eID	Operations: reading all data groups User interaction: CAN for PACE	Operations: writing a subset of data groups; reading all or a subset of data groups User interaction: eID-PIN or eID-PUK or CAN[25] for PACE	-
eSign	-	Operations: activating eSign application User interaction: eID-PIN or eID-PUK or CAN[25] for PACE In the eSign context, the current terminal is equivalent to CGA in [7]	Operations: generating digital signatures User interaction: CAN for PACE, then eSign-PIN for access to the signature function In the eSign context, the current terminal is equivalent – as a general term – to SCA and HID in [7]

Table 1: ID_Card applications vs. terminal types

[25] if the terminal indicates such required authorisation with PACE (an official terminal), see C.4.2 in [11]

2 Conformance Claims

2.1 CC Conformance Claim

24 This protection profile claims conformance to

– Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
– Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]
– Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

25 The

– Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [4]

has to be taken into account.

2.2 PP Claim

26 This PP claims *strict* conformance to 'Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-1:2009, ver. 1.03, 2009-12, BSI-CC-PP-0059' [7].

27 *Application note 8:* This conformance claim covers the part of the security policy for the *eSign* application of the TOE corresponding to the security policy defined in [7] and, hence, is applicable, if the *eSign* application is operational. In addition to [7], the current PP specifies authentication and communication protocols (PACE, terminal authentication, passive authentication, chip authentication) having to be used for the *eSign* application of the TOE. These protocols contribute to securing SVD-export, DTBS-import and VAD-import functionality.

28 *Application note 9:* The eSign application of the TOE is intended to generate advanced or qualified electronic (concretely: digital) signatures. The main specific property distinguishing qualified electronic signatures is that they base on qualified certificates[26] and are created by secure signature creation devices (SSCD).
Since the current TOE (its part the eSign application) shall be used as SSCD due to the PP conformance claim above, the only specific difference remained is using qualified certificates for qualified signatures. Whether a certificate is qualified or not is a pure organisational issue from the point of view of the TOE which does not impact the TOE functionality. Therefore, the PP conformance claim above covers not only qualified signatures, but can also do this for advanced signatures under an appropriate interpretation of the organisational security policies P.CSP_QCert and P.QSign in [7].

[26] being valid at signature creation time

29 The part of the security policy for the *ePassport* application of the TOE is contextually in a tight connection with the protection profile 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009' [6], however does not claim any formal conformance to it. The main reason for this decision is that the current PP does not cover BAC. Besides this, it cannot be ensured for the future, that the specifications [10] and [11] remain compatible to each other. In addition to the security policy defined in [6], the *ePassport* application of the TOE uses PACE as the mandatory communication establishment protocol.

2.3 Package Claim

30 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 as defined in the CC, part 3 [3].

2.4 Conformance Claim Rationale

31 *Application note 10:* The current PP claims *strict* conformance to the protection profile SSCD Core PP [7] as required there in sec. 6.4. The part of the security policy for the ePassport application of the TOE is contextually in a tight connection with the ICAO EAC PP [6]. Due to this fact, it is sensible to distinguish between separated sets of {TOE type, SPD statement, security objectives statement, security requirements statement} for each application residing in the TOE: ePassport, eID and eSign, respectively[27], unless the items are identical or hierarchical as in the case of the SARs.
The author of the current PP will mark item's belonging to each TOE's application off.

2.4.1 'Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation'

TOE Type

32 The TOE type stated in [7], sec. 5.4.2 is '… a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory'.

33 This TOE type is obviously commensurate with the current TOE type in the part being provided by the eSign application, see sec. 1.2.1 and 1.2.3 above.

SPD Statement

34 The security problem definition (SPD) of the current PP contains the security problem definition of the PP [7]. The current SPD includes the same threats, organisational security policies and assumptions as for the TOE in [7] and comprehends several additional items as stated in chap. 3 below.

[27] see Application notes in sec. 2.2

35 *Application note 11:* Strict conformance presumes that assumptions of the current PP shall be identical to the assumptions of each PP to which the conformance is being claimed. As explained in the *Application note 10* above, the assumptions for the current PP might consist of three blocks: assumptions for the ePassport, for the eID and assumptions for the eSign application.
In this context, the current assumptions block for the eSign application is identical to the assumptions from [7].

Security Objectives Statement

36 The security objectives statement for the TOE in the current PP includes all the security objectives for the TOE of the PP [7] and comprehends several additional items as stated in chap. 4.1 below.

37 The security objectives statement for the TOE’s operational environment in the current PP includes all security objectives for the operational environment of the PP [7] and comprehends several additional items as stated in chap. 4.2 below.

38 *Application note 12:* Strict conformance presumes that the security objectives for the operational environment of the current PP shall be identical to those items of each PP to which the conformance is being claimed (unless a re-assignment according to [1], sec. 9.3). As explained in the *Application note 10* above, the security objectives for the operational environment for the current PP might consist of three blocks: objectives for the ePassport, for the eID and objectives for the eSign application.
In this context, the current block of environmental objectives for the eSign application is identical to the equivalent objectives from [7].

Security Requirements Statement

39 The SFR statement for the TOE in the current PP includes all the SFRs for the TOE of the PP [7] and comprehends several additional items as stated in chap. 6.1 below.

40 The SAR statement for the TOE in the current PP includes all the SARs for the TOE of the PP [7] as stated in chap. 6.2 below. The current assurance package contains the assurance components ALC_DVS.2 and ATE_DPT.2 being hierarchical to ALC_DVS.1 respectively ATE_DPT.1 as required by [7].

41 *Application note 13:* Strict conformance allows that the security requirements for the TOE of the current PP may be hierarchically stronger than those items of each PP to which the conformance is being claimed.

2.5 Conformance statement

42 This PP requires *strict* conformance of any ST or PP claiming conformance to this PP.

3 Security Problem Definition

43 *Application note 14:* Since the current PP covers three different applications – ePassport, eID and eSign –, the author decided to trace the belonging of each formal item within the set of {SPD statement, security objectives statement, security requirements statement} to the respective application; cf. also the *Application note 10* in sec. 2.4 above.

3.1 Introduction

Assets

44 The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap. 7 for the term definitions)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
ePassport, eID, eSign			
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the applications of the ID_Card as defined in [11] and (i) being allowed to be *read out*	Confidentiality[30] Integrity Authenticity

[28] Since the Restricted Identification according to [11], sec. 4.5 represents just a functionality of the ID_Card, the key material needed for this functionality and stored in the TOE is treated here as User Data in the sense of the CC.

[29] SCD in [7]

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
		or *written* solely by an authenticated terminal (in the sense of [11], sec. 3.2) respectively (ii) being allowed to be *used* solely by an authenticated terminal (in the sense of [11], sec. 3.2) (the private Restricted Identification key[28]) respectively (iii) being allowed to be *used* solely by the authenticated ID_Card holder (the private signature key within the eSign application[29]). This asset covers 'User Data on the MRTD's chip' and 'Logical MRTD sensitive User Data' in [6] as well as 'SCD' and 'DTBS/R' in [7].	
2	user data transferred between the TOE and the service provider connected[31]	All data (being not authentication data) being transferred in the context of the applications of the ID_Card as defined in [11] between the TOE and an authenticated terminal (in the sense of [11], sec. 3.2). User data can be received and sent (exchange ⇔ {receive, send}). This asset covers 'DTBS' in [7].	Confidentiality[32] Integrity Authenticity
3	ID_Card tracing data	Technical information about the current and previous locations of the ID_Card gathered by inconspicuous (for the ID_Card holder) recognising the TOE knowing *neither* CAN *nor* MRZ *nor* eID-PIN *nor* eID-PUK. TOE tracing data can be provided / gathered.	unavailability[33]

[30] Though not each data element stored on the TOE represents a secret, the specification [11] anyway requires securing their confidentiality: only terminals authenticated according to [11], sec. 4.4 can get access to the user data stored.

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

[32] Though not each data element being transferred represents a secret, the specification [11] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [11], sec. 4.3.2, 4.4.2.

Table 2: Primary assets

45 *Application Note 15*: Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the ID_Card holder which also include his sensitive (biometrical) data. Hence, the general security policy defined by the current PP also secures these specific ID_Card holder's data as stated in the table above.

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

47 The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	Asset	Definition	Property to be maintained by the current security policy
ePassport, eID, eSign			
4	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [6].	Availability
6	TOE immanent secret cryptographic keys	Secret cryptographic material used by the TOE in order to enforce its security functionality[34].	Confidentiality Integrity
7	TOE immanent non-secret cryptographic material	Non-secret cryptographic (public) keys and other non-secret material (Card Security Object containing digital signature) used by the TOE in order to enforce its security functionality. This asset also covers 'SVD' in [7].	Integrity Authenticity
8	Secret ID_Card holder authentication data	Secret authentication information for the ID_Card holder being used for verification of the authentication attempts as authorised ID_Card holder (– eID-PIN and eID-PUK[35] stored in the ID_Card as well as	Confidentiality Integrity

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

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

[35] eID-PIN and eID-PUK are global secrets being valid for the entire ID_Card.

Object No.	Asset	Definition	Property to be maintained by the current security policy
		– eSign-PIN (and eSign-PUK, if any)[36] (i) stored in the ID_Card[37] and (ii) transferred to it[38])	
9	ID_Card communication establishment authorisation data	Restricted-revealable[39] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (CAN for ePassport, eID, eSign; MRZ for ePassport). These data are stored in the TOE and are not to convey to it.	Confidentiality[39] Integrity

Table 3: Secondary assets

48 *Application Note 16*: ID_Card holder authentication and ID_Card communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authentication/authorisation attempt.
The TOE shall secure the reference information as well as – together with the terminal connected[40] – the verification information in the 'TOE <-> terminal' channel, if it has to be transferred to the TOE. Please note that CAN, MRZ, eID-PIN and eID-PUK are not to convey to the TOE.

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

Subjects and external entities

50 This protection profile considers the following subjects:

External Entity No.	Subject No.	Role	Definition
1	1	ID_Card holder	A person for whom the ID_Card Issuer has personalised the ID_Card[41]. This subject is commensurate with 'MRTD Holder' in [6] and 'Signatory' in [7]. Please note that an ID_Card holder can also be an attacker (s. below).
2	-	ID_Card presenter	A person presenting the ID_Card to a terminal[42]

[36] eSign-PIN (and eSign-PUK, if any) are local secrets being valid only within the eSign application.

[37] is commensurate with RAD in [7]

[38] is commensurate with VAD in [7]

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

[40] the input device of the terminal

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

External Entity No.	Subject No.	Role	Definition
			and claiming the identity of the ID_Card holder. This subject is commensurate with 'Traveller' in [6] and 'User' in [7]. Please note that an ID_Card presenter can also be an attacker (s. below).
3	-	Service Provider (SP)	An official or commercial organisation providing services which can be used by the ID_Card holder. Service Provider uses rightful terminals managed by a DV.
4	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as neither PCT nor EIS nor ATT nor SGT ('Terminal' is used by the ID_Card presenter). This subject is commensurate with 'Terminal' in [6].
5	3	PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the ID_Card and the related value presented to the terminal by the ID_Card presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ID_Card using a shared password (CAN, eID-PIN, eID-PUK or MRZ). The PCT is not allowed reading User Data (see sec. 4.2.2 in [11]). See also *Application note 4* and par. 23 above and [11], chap. 3.3, 4.2, table 1.2 and G.2
6	4	Inspection system (EIS)	A technical system being used by an authority[43] and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ID_Card presenter as the ID_Card holder (for *ePassport*: by comparing the real biometrical data of the ID_Card presenter with the stored biometrical data of the ID_Card holder). An Inspection System is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorised by the ID_Card Issuer through the Document Verifier of the receiving State (by issuing terminal certificates) to read a subset of the data stored on the ID_Card. The Inspection System in the context of [11] (and of

[42] in the sense of [11]

[43] concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			the current PP) is commensurate with the Extended Inspection System (EIS) as defined in [6]. See also *Application note 4* and par. 23 above and [11], chap. 3.2 and C.4.
7	5	Authentication Terminal (ATT)	A technical system being operated and used either by a governmental organisation (Official Domestic Document Verifier) or by any other, also commercial organisation and (i) verifying the ID_Card presenter as the ID_Card holder (using secret eID-PIN[44]), (ii) updating a subset of the data of the eID application and (iii) activating the eSign application. An Authentication Terminal is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorised by the ID_Card Issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset of the data stored on the ID_Card. See also par. 23 above and [11], chap. 3.2 and C.4.
8	6	Signature Terminal (SGT)	A technical system used for generation of digital signatures. A Signature Terminal is a PCT additionally supporting the Chip Authentication (incl. passive authentication) and the Terminal Authentication protocols and is authorised by the ID_Card Issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset of the data stored on the ID_Card. See also par. 23 above and [11], chap. 3.2 and C.4.
9	7	Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (governmental or commercial organisation) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [11], chap. 2.2.2. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ID_Card Issuer; a foreign DV is acting under a policy of the

[44] secret eID-PUK can be used for unblocking the eID-PIN as well as the eSign-PIN and resetting the related retry counters.

External Entity No.	Subject No.	Role	Definition
			respective foreign CVCA (in this case there shall be an appropriate agreement[45] between the ID_Card Issuer und a foreign CVCA ensuring enforcing the ID_Card Issuer's privacy policy[46]). This subject is commensurate with 'Document Verifier' in [6].
10	8	Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the ID_Card Issuer with respect to protection of user data stored in the ID_Card (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the rightful terminals (EIS, ATT, SGT) and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [11], chap. 2.2.1. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [8]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [11], sec. 2.2.1. This subject is commensurate with 'Country Verifying Certification Authority' in [6].
11	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Card Security Object stored on the ID_Card for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [11], chap. 1.1 and [8]. This role is usually delegated to a Personalisation Agent.
12	-	Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ID_Card Issuer with respect to confirming correctness of user and TSF data stored in the ID_Card. The CSCA represents the country specific root of the PKI for the ID_Cards and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [8], 5.1.1.

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

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

External Entity No.	Subject No.	Role	Definition
			The Country Signing Certification Authority issuing certificates for Document Signers (cf. [8]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [11], sec. 2.2.1.
13	-	Certification Service Provider (CSP)	An organisation issuing certificates and providing other services related to electronic signatures. There can be 'common' and 'qualified' CSP: A 'qualified' Certification Service Provider can also issue qualified certificates[47]. A CSP is the Certification Service Provider in the sense of [7].
14	9	Personalisation Agent	An organisation acting on behalf of the ID_Card Issuer to personalise the ID_Card for the ID_Card holder by some or all of the following activities: (i) establishing the identity of the ID_Card holder for the biographic data in the ID_Card[48], (ii) enrolling the biometric reference data of the ID_Card holder[49], (iii) writing a subset of these data on the physical Identification Card (optical personalisation) and storing them in the ID_Card (electronic personalisation) for the ID_Card holder as defined in [11], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card Security Object defined in [11] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the ID_Card Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role. This subject is commensurate with 'Personalisation agent' in [6] and 'Administrator' in [7].
15	10	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the ID_Card Manufacturer completing the IC to the ID_Card. The Manufacturer is the default user of the TOE during the manufacturing life phase[50]. The TOE itself does not distinguish between the IC Manufacturer and ID_Card Manufacturer using this role Manufacturer.

[47] cf. *Application note 9* in sec. 2.2 above.

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

[49] relevant for the ePassport application

[50] cf. also par. 14 in sec. 1.2.3 above

External Entity No.	Subject No.	Role	Definition
			This subject is commensurate with 'Manufacturer' in [6].
16	-	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 having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This subject is commensurate with 'Attacker' in [6] and in [7].

Table 4: Subjects and external entities[51]

51 *Application Note 17*: Since the TOE does not support BAC, a Basic Inspection System (BIS) cannot be recognised by the TOE, see *Application note 4* above.

3.2 Threats

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

53 The following threats are defined in the current PP (they are derived from the ICAO-BAC PP [5] and ICAO-EAC PP [6]):

54 **T.Skimming** **Skimming ID_Card / capturing card-terminal communication**

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

Application Note 18: A product supporting BAC cannot avert this threat in the context of the security policy defined in this PP, see also the *Application note 4* above.

[51] This table defines external entities and subjects in the sense of [1]. Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

Application Note 19: This threat also covers the item T.Read_Sensitive_Data in the ICAO-EAC PP [6]: Sensitive biometric reference data stored on the ID_Card are part of the asset *user data stored on the TOE*. Knowledge of the Document Basic Access Keys is here not applicable, because the TOE does not support the BAC protocol and, therefore, the Document Basic Access Keys are not existent for the TOE.

55 *Application Note 20*: MRZ is printed and CAN is printed or stuck on the Identification Card. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.ID_Card-Holder.

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

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

Application Note 21: A product supporting BAC cannot avert this threat in the context of the security policy defined in this PP, see also the *Application note 4* above.

57 **T.ID_Card_Tracing** **Tracing ID_Card**

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

Application Note 22: A product supporting BAC cannot avert this threat in the context of the security policy defined in this PP, see also the *Application note 4* above.

58 **T.Counterfeit** **Counterfeiting ID_Card**

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

Application Note 23: A product supporting BAC cannot avert this threat in the context of the security policy defined in this PP, see also the *Application note 4* above.

59 **T.Forgery** **Forgery of Data**

An attacker fraudulently alters the User Data or/and TSF-data stored on the ID_Card or/and exchanged between the TOE and the Service Provider connected in order to outsmart the authenticated terminal (EIS, ATT or SGT) by means of changed ID_Card holder's related reference data (like biographic or biometric data or SCD/SVD). The attacker does it in such a way that the Service Provider (represented by the terminal connected) perceives these modified data as authentic one.
This item concerns the following application(s): ePassport, eID, eSign.

This threat partially covers T.SVD_Forgery (only stored, but not being sent to the CGA SVD) from Table 5.

60 **T.Abuse-Func** **Abuse of Functionality**

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclosure the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the ID_Card holder.
This item concerns the following application(s): ePassport, eID, eSign.
This threat covers T.SigF_Misuse from Table 5.

Application Note 24: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

61 **T.Information_Leakage** **Information Leakage from ID_Card**

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data. The information leakage may be inherent in the normal operation or caused by the attacker.
This item concerns the following application(s): ePassport, eID, eSign.

Application Note 25: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

62 **T.Phys-Tamper** **Physical Tampering**

An attacker may perform physical probing of the ID_Card in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the ID_Card in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the ID_Card.
This item concerns the following application(s): ePassport, eID, eSign.
This threat covers T.Hack_Phys from Table 5.

Application Note 26: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the ID_Card) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the ID_Card's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

63 **T.Malfunction** **Malfunction due to Environmental Stress**

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

Application note 27: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

64 The current PP also includes all threats of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational.

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

Threat identifier	Comments
	– eSign

Table 5: Threats taken over from [7]

3.3 Organisational Security Policies

65 The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operation.

66 **P.Pre-Operational** **Pre-operational handling of the ID_Card**

1) The ID_Card Issuer issues the ID_Cards and approves using the terminals complying with all applicable laws and regulations.

2) The ID_Card Issuer guarantees correctness of the user data (amongst other of those, concerning the ID_Card holder) and of the TSF-data permanently stored in the TOE[52].

3) The ID_Card Issuer uses only such TOE's technical components (IC) which enable traceability of the ID_Cards in their manufacturing and issuing life phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 above.

4) If the ID_Card Issuer authorises a Personalisation Agent to personalise the ID_Cards for ID_Card holders, the ID_Card Issuer has to ensure that the Personalisation Agent acts in accordance with the ID_Card Issuer's policy.

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

67 **P.ID_Card_PKI** **PKI for Chip and Passive Authentication (issuing branch)[53]**

Application Note 28: The description below states responsibilities of the involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1) The ID_Card Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the ID_Card. For this aim he runs a Country Signing Certification Authority (CSCA). The ID_Card Issuer shall make the CSCA Certificate (C_{CSCA}) and the Document Signer Certificates (C_{DS}) available to the CVCAs under agreement[54] (who shall finally distribute them to their rightful terminals).

2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be

[52] cf. Table 2 and Table 3 above

[53] Passive authentication is considered to be part of the chip authentication protocol within this PP.

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

made available to the ID_Card Issuer by strictly secure means, see [8], 5.1.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the ID_Card Issuer, see [8], 5.1.1.

3) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret, (iv) securely use the Document Signer Private Key for signing the Card Security Objects of ID_Cards and (v) manage Chip Authentication Key Pairs {SK_{PICC}, PK_{PICC}} used for the chip authentication as defined in [11], sec. 4.3.[55]

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

68 **P.Terminal_PKI PKI for Terminal Authentication (receiving branch)**

Application Note 29: The description below states responsibilities of the involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1) The ID_Card Issuer shall establish a public key infrastructure for the card verifiable certificates used for terminal authentication. For this aim, the ID_Card Issuer shall run a domestic Country Verifying Certification Authority (domestic CVCA) and may use already existing foreign CVCAs[56]. The ID_Card Issuer shall make the CVCA Link Certificate available to the CSCA (who shall finally distribute it to its ID_Cards).

2) A CVCA shall securely generate, store and use the CVCA key pair. A CVCA shall keep the CVCA Private Key secret and issue a self-signed CVCA Certificate (C_{CVCA}) having to be made available to the ID_Card Issuer by strictly secure means as well as to the respective Document Verifiers. A CVCA shall create the Document Verifier Certificates for Document Verifier Public Keys (C_{DV}) and distribute them back to the respective Document Verifiers[57].

3) A Document Verifier shall (i) generate the Document Verifier Key Pair, (ii) hand over the Document Verifier Public Key to the CVCA for certification, (iii) keep the Document Verifier Private Key secret and (iv) securely use the Document Verifier Private Key for signing the Terminal Certificates (C_T) of the terminals being managed by him. The Document Verifier shall make C_T, C_{DV} and C_{CVCA} available to the respective Service Provider (who puts them in his terminals)[58].

4) A Service Provider shall (i) generate the Terminal Authentication Key Pairs {SK_{PCD}, PK_{PCD}}, (ii) hand over the Terminal Authentication Public Keys (PK_{PCD}) to the DV for

[55] A Document Signer shall also manage Restricted Identification Key Pairs {SK_{ID}, PK_{ID}} [11], sec. 2.3 and 4.5. The private Restricted Identification Key SK_{ID} shall be stored in the TOE, whereby the public Restricted Identification Key PK_{ID} – in a database of the DS. See also *Application note 6* and Table 2, object #1.

[56] In this case there shall be an appropriate agreement between the ID_Card Issuer und a foreign CVCA ensuring enforcing the ID_Card Issuer's privacy policy. Existence of such an agreement may technically be reflected by means of issuing a C_{CVCA-F} for the Public Key of the foreign CVCA signed by the domestic CVCA.

[57] A CVCA shall also manage a Revocation Sector Key Pair {$SK_{Revocation}$, $PK_{Revocation}$} [11], sec. 2.3 and 4.5. For Restricted Identification please see *Application note 6* and Table 2, object #1.

[58] A DV shall also manage Sector's Static Key Pairs {$SK_{SectorNN}$, $PK_{SectorNN}$} [11], sec. 2.3 and 4.5. For Restricted Identification please see *Application note 6* and Table 2, object #1.

certification, (iii) keep the Terminal Authentication Private Keys (SK_{PCD}) secret, (iv) securely use the Terminal Authentication Private Keys for the terminal authentication as defined in [11], sec. 4.4 and (v) install C_T, C_{DV} and C_{CVCA} in the rightful terminals operated by him.

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

69 **P.Trustworthy_PKI** **Trustworthiness of PKI**

1) The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Card Security Objects having to be stored on the ID_Cards.

2) CVCAs shall ensure that they issue their certificates exclusively to the rightful organisations (DV) and DVs shall ensure that they issue their certificates exclusively to the rightful equipment (terminals)[59].

3) CSPs shall ensure that they issue their certificates exclusively for the rightful data (public signature key of the ID_Card holder)[60].

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

70 **P.Terminal** **Abilities and trustworthiness of rightful terminals**

1) Rightful terminals (inspection system, authentication terminal and signature terminal, cf. Table 1 above) shall be used by Service Providers and by ID_Card holders as defined in [11], sec. 3.2.

2) They shall implement the terminal parts of the PACE protocol [11], sec. 4.2, of the Terminal Authentication protocol [11], sec. 4.4, of the Passive Authentication [11], sec. 3.4 and of the Chip Authentication protocol [11], sec. 4.3[61] and use them in this order[62]. A rightful terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) Rightful terminals shall store the related credentials needed for the terminal authentication (terminal authentication key pair $\{SK_{PCD}, PK_{PCD}\}$ and the terminal certificate (C_T) over PK_{PCD} issued by the DV related as well as C_{DV} and C_{CVCA}; the terminal certificate includes an authorisation mask (CHAT) for access to the data stored on the ID_Card) in order to enable and to perform the terminal authentication as defined in [11], sec. 4.4.

4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of PK_{PICC}, [11], sec. 4.3.1.2).

---

59 This rule is relevant for T.Skimming

60 This property is affine to P.CSP_QCert from [7].

61 The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within this PP.

62 This order is only commensurate with the branch rightmost in Fig. 3.1, sec. 3.1.1 of [11]. Other branches of this figure are not covered by the security policy of the current PP.

5) A rightful terminal must not send assets (e.g. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the Chip Authentication after the Terminal Authentication[63].

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

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

71 The current PP also includes all OSPs of the SSCD PP [7] (please regard the *Application note 9* above). These items are applicable, if the *eSign* application is operational.

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

Table 6: OSPs taken over from [7]

3.4 Assumptions

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

73 The current PP includes all assumptions of the SSCD PP [7] (please regard the *Application note 11* and Table 1 above). These items are applicable, if the *eSign* application is operational.

Assumption identifier	Comments
A.CGA	This item concerns not only qualified, but also non-qualified certificates, cf. *Application note 9* above –

[63] This rule is relevant for T.Skimming

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

Table 7: Assumptions taken over from [7]

74 The current PP does not include any additional assumptions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

77 **OT.Data_Integrity Integrity of Data**

The TOE must ensure integrity of the User Data and the TSF-data[64] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).
The TOE must ensure integrity of the User Data and the TSF-data[64] during their exchange between the TOE and the Service Provider connected (and represented by either EIS or ATT or SGT) after the Terminal- and the Chip Authentication.
This item concerns the following application(s): ePassport, eID, eSign.

78 **OT.Data_Authenticity Authenticity of Data**

The TOE must ensure authenticity of the User Data and the TSF-data[65] stored on it by enabling verification of their authenticity at the terminal-side[66].
The TOE must ensure authenticity of the User Data and the TSF-data[65] during their exchange between the TOE and the Service Provider connected (and represented be either EIS or ATT or SGT) after the Terminal- and the Chip Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[67].
This item concerns the following application(s): ePassport, eID, eSign.

79 **OT.Data_Confidentiality Confidentiality of Data**

The TOE must ensure confidentiality of the User Data and the TSF-data[68] by granting read access only to authorised rightful terminals (EIS, ATT, SGT) according to the effective terminal authorisation level (CHAT) presented by the terminal connected[69].
The TOE must ensure confidentiality of the User Data and the TSF-data[68] during their

[64] where appropriate, see Table 3 above

[65] where appropriate, see Table 3 above

[66] verification of SO_C

[67] secure messaging after the chip authentication, see also [11], sec. 4.4.2

[68] where appropriate, see Table 3 above

[69] The authorisation of the terminal connected (CHAT) is drawn from the terminal certificate chain used for the successful terminal authentication as defined in [11], sec. 4.4 and shall be a non-strict subset of the authorisation defined in the Terminal Certificate (C_T), the Document Verifier Certificate (C_{DV}) and the C_{CVCA} in the certificate chain up to the Country Verifying Certification Authority of the ID_Card Issuer (receiving PKI branch of the ID_Card Issuer). The effective terminal authorisation can additionally be restricted by the ID_Card holder by a respective input at the terminal.

exchange between the TOE and the Service Provider connected (and represented be either EIS or ATT or SGT) after the Terminal- and the Chip Authentication.
This item concerns the following application(s): ePassport, eID, eSign.

80 **OT.ID_Card_Tracing Tracing ID_Card**

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

81 **OT.Chip_Auth_Proof Proof of ID_Card authenticity**

The TOE must enable the terminal connected to verify the authenticity of the ID_Card as a whole device as issued by the ID_Card Issuer (issuing PKI branch of the ID_Card Issuer) by means of the Passive and Chip Authentication as defined in [11], sec. 4.3.
This item concerns the following application(s): ePassport, eID, eSign.

Application note 30: The OT.Chip_Auth_Proof implies the ID_Card's chip to have a unique secret to prove its authenticity by knowledge, i.e. a Chip Authentication Private Key as TSF-data.
The terminal shall have the reference data to verify the authentication attempt of the ID_Card's chip, i.e. a certificate for the respective Chip Authentication Public Key (PK_{PICC}) fitting to the Chip Authentication Private Key (SK_{PICC}). This certificate is provided by (i) the Chip Authentication Public Key stored on the TOE and (ii) the hash value of this PK_{PICC} in the Card Security Object (SO_C) signed by the Document Signer.

82 **OT.Prot_Abuse-Func Protection against Abuse of Functionality**

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

83 **OT.Prot_Inf_Leak Protection against Information Leakage**

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

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

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

Application note 31: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

84 **OT.Prot_Phys-Tamper Protection against Physical Tampering**

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

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

with a prior

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

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

85 **OT.Prot_Malfunction Protection against Malfunctions**

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

86 The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment.*

87 **OT.Identification Identification of the TOE**

The TOE must provide means to store Initialisation[70] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life phases of the ID_Card.
This item concerns the following application(s): ePassport, eID, eSign.

88 **OT.Personalisation Personalisation of ID_Card**

The TOE must ensure that the user data (amongst other those concerning the ID_Card holder[71]) and the TSF-data permanently stored in the TOE can be written by authorised Personalisation Agents only. The Card Security Object can be updated by authorised Personalisation Agents (in the role of DS), if the related data have been modified. The optional *eSign* application can additionally be activated on the TOE on behalf of the CSP issuing this *eSign* application, if the ID_Card holder had applied for this.
This item concerns the following application(s): ePassport, eID, eSign.

[70] amongst other, IC Identification data

[71] biographical and biometrical data as well as the SCD, if the *eSign* is operational.

89 The current PP also includes all security objectives for the TOE of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational.

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

Table 8: TOE objectives taken over from [7]

4.2 Security Objectives for Operational Environment

I. ID_Card Issuer as the general responsible

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

91 **OE.Legislative_Compliance**

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

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

92 The ID_Card Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the *Application Note 28* above):

93 **OE.Passive_Auth_Sign Authentication of ID_Card by Signature**

The ID_Card Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the ID_Card Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) make the Certificate of the CSCA Public Key (C_{CSCA}) and the Document Signer Certificates (C_{DS}) available to the ID_Card Issuer, who makes them available to his own (domestic) CVCA as well as to the foreign CVCAs under agreement[72]. Hereby authenticity and integrity of these certificates are being maintained.
A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Card Security Objects of genuine ID_Cards in a secure operational environment only. The digital signature in the Card Security Object relates to all security information objects according to [11], Appendix A.
The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Card Security Objects having to be stored on ID_Cards. This item concerns the following application(s): ePassport, eID.
This item also covers OE.CGA_SSCD and partially OE.SVD_Auth from Table 9 below for the eSign application.

94 **OE.Chip_Auth_Key Chip Authentication Key**

A Document Signer acting in accordance with the CSCA policy has to (i) generate the ID_Card's Chip Authentication Key Pair $\{SK_{PICC}, PK_{PICC}\}$ used for the chip authentication as defined in [11], sec. 4.3, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key Info (Appendix A of [11]) and (iii) support Service Providers to verify the authenticity of the ID_Card's chips used for genuine ID_Cards by certification of the Chip Authentication Public Key by means of the Card Security Object.

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

A Document Signer has also to manage Restricted Identification Key Pairs $\{SK_{ID}, PK_{ID}\}$ [11], sec. 2.3 and 4.5: the private Restricted Identification Key SK_{ID} is to store in the TOE, whereby the public Restricted Identification Key PK_{ID} – in a database of the DS. See also *Application note 6* and Table 2, object #1.
This item concerns the following application(s): ePassport, eID.
This item also covers OE.CGA_SSCD and partially OE.SVD_Auth from Table 9 below for the eSign application.

95 **OE.Personalisation Personalisation of ID_Card**

The ID_Card Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the ID_Card holder and create the biographical data for the ID_Card[73], (ii) enrol the biometric reference data of the ID_Card holder[74], (iii) write a subset of these data on the physical Identification Card (optical personalisation) and store them in the ID_Card (electronic personalisation) for the ID_Card holder as defined in [11], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Card Security Object defined in [8] (in the role of a DS).
This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.CGA_QCert from Table 9 below for the eSign application.

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

96 The ID_Card Issuer and the related domestic CVCA as well as the foreign CVCAs under agreement (with the ID_Card Issuer)[75] will implement the following security objectives for the TOE environment (see also the *Application Note 29* above):

97 **OE.Terminal_Authentication Authentication of rightful terminals**

The ID_Card Issuer has to establish the necessary public key infrastructure as follows: the domestic CVCA acting on behalf and according to the policy of the ID_Card Issuer as well as each foreign CVCA acting under agreement with the ID_Card Issuer and according to its policy must (i) generate a cryptographically secure CVCA Key Pair, (ii) ensure the secrecy of the CVCA Private Key and sign Document Verifier Certificates in a secure operational environment, (iii) make the Certificate of the CVCA Public Key (C_{CVCA}) available to the ID_Card Issuer (who make it available to his own CSCA[76]) as well as to the respective Document Verifiers, (iv) distribute Document Verifier Certificates (C_{DV}) back to the respective Document Verifiers. Hereby authenticity and integrity of these certificates are being maintained. A CVCA has also to manage a Revocation Sector Key Pair $\{SK_{Revocation}, PK_{Revocation}\}$ [11], sec. 2.3 and 4.5[77].
A Document Verifier acting in accordance with the respective CVCA policy must (i) generate a cryptographically secure Document Verifying Key Pair, (ii) ensure the secrecy of the Document Verifying Private Key, (iii) hand over the Document Verifier Public Key to the respective CVCA for certification, (iv) sign the Terminal Certificates (C_T) of the terminals being managed by him in a secure operational environment only, and (v) make C_T, C_{DV} and C_{CVCA} available to

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

[74] relevant for the ePassport application

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

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

[77] For Restricted Identification please see *Application note 6* and Table 2, object #1

the respective Service Providers operating the terminals certified. This certificate chain contains, amongst other, the authorisation level of pertained terminals for differentiated data access on the ID_Card. A DV has also to manage Sector's Static Key Pairs $\{SK_{SectorNN}$, $PK_{SectorNN}\}$ [11], sec. 2.3 and 4.5[78].
A Service Provider participating in this PKI (and, hence, acting in accordance with the policy of the related DV) must (i) generate Terminal Authentication Key Pairs $\{SK_{PCD}$, $PK_{PCD}\}$, (ii) ensure the secrecy of Terminal Authentication Private Keys, (iii) hand over the Terminal Authentication Public Keys $\{PK_{PCD}\}$ to the DV for certification, (iv) securely use the Terminal Authentication Private Keys for the terminal authentication as defined in [11], sec. 4.4 and (v) install C_T, C_{DV} and C_{CVCA} in the rightful terminals operated by him.
CVCAs must issue their certificates exclusively to the rightful organisations (DV) and DVs must issue their certificates exclusively to the rightful equipment (terminals)[79].
This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.SVD_Auth from Table 9 below for the eSign application.

98 **OE.Terminal** **Terminal operating**

The Service Providers participating in the current PKI (and, hence, acting in accordance with the policy of the related DV) must operate their terminals as follows:

1) They use their terminals (inspection systems, authentication or signature terminals, cf. Table 1 above) as defined in [11], sec. 3.2.

2) Their terminals implement the terminal parts of the PACE protocol [11], sec. 4.2, of the Terminal Authentication protocol [11], sec. 4.4, of the Passive Authentication [11], sec. 3.4 (by verification of the signature of the Card Security Object) and of the Chip Authentication protocol [11], sec. 4.3[80] and use them in this order[81]. A rightful terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) Their terminals securely store the related credentials needed for the terminal authentication (terminal authentication key pair $\{SK_{PCD}$, $PK_{PCD}\}$ and the terminal certificate (C_T) over PK_{PCD} issued by the DV related as well as C_{DV} and C_{CVCA}; the terminal certificate includes the authorisation mask (CHAT) for access to the data stored on the ID_Card) in order to enable and to perform the terminal authentication as defined in [11], sec. 4.4.

4) Their terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the ID_Card (determination of the authenticity of PK_{PICC}, [11], sec. 4.3.1.2).

[78] For Restricted Identification please see *Application note 6* and Table 2, object #1.

[79] This rule is relevant for T.Skimming

[80] The Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within this PP

[81] This order is only commensurate with the branch rightmost in Fig. 3.1, sec. 3.1.1 of [11]. Other branches of this figure are not covered by the security policy of the current PP.

5) Their terminals must not send assets (e.g. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the Chip Authentication after the Terminal Authentication[82].

6) Their terminals and its environment must ensure confidentiality and integrity of respective data handled by it (e.g. confidentiality of PINs/PUKs, integrity of PKI certificates and DTBS, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.CGA_TC_SVD, OE.HID_TC_VAD, OE.SCA_TC_DTBS, OE.SVD_Auth, OE.DTBS_Intend from Table 9 below for the eSign application.

IV. ID_Card holder Obligations

99 **OE.ID_Card-Holder** **ID_Card holder Obligations**

The ID_Card Holder has to keep his or her verification values of eID-PIN and eID-PUK secret. The ID_Card Holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.

This item concerns the following application(s): ePassport, eID.
This item also partially covers OE.Signatory from Table 9 below for the eSign application.

100 The current PP also includes all security objectives for the TOE's environment of the SSCD PP [7] (please regard the *Application note 12* and Table 1 above). These items are applicable, if the *eSign* application is operational.

Objective identifier	Comments
OE.SVD_Auth	concerns the following application(s): – eSign
OE.CGA_QCert	enforces the property #3 (CSP duties) of P.Trustworthy_PKI concerns the following application(s): – eSign
OE.DTBS_Intend	concerns the following application(s): – eSign

[82] This rule is relevant for T.Skimming

Objective identifier	Comments
OE.Signatory	concerns the following application(s): – eSign
OE.SSCD_Prov_Service	concerns the following application(s): – eSign This environmental objective shall be achieved in such a way that (i) the CSP checks by means of the CGA, whether the device presented by the applicant for the (qualified) certificate examples holds unique identification as SSCD and is able to prove this identity; (ii) CGA detects alteration of the SVD imported from the TOE and verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the (qualified) certificate.
OE.HID_VAD	concerns the following application(s): – eSign This environmental objective shall be achieved in such a way that HID provides the human interface for user authentication and HID ensures confidentiality of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.
OE.DTBS_Protect	concerns the following application(s): – eSign This environmental objective shall be achieved in such a way that SCA provides a

Objective identifier	Comments
	trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS-representation cannot be altered undetected in transit between the SCA and the TOE.

Table 9: TOE's environment objectives taken over from [7]

4.3 Security Objective Rationale

101 The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and *necessity* of the objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	OT.Identification	OT.Personalisation	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Personalisation	OE.Passive_Auth_Sign	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Terminal	OE.ID_Card-Holder	OE.Legislative_Compliance	OE.CGA_QCert ([7])[83]
T.Skimming			x	x	x										x	x	x		
T.Eavesdropping					x														
T.ID_Card_Tracing						x											x		
T.Forgery		x	x	x				x		x			x			x			
T.Counterfeit							x							x		x			
T.Abuse-Func								x											
T.Information_Leakage									x										
T.Phys-Tamper										x									
T.Malfunction											x								
P.Pre-Operational	x	x										x						x	

83 This item is applicable, if the *eSign* application is operational.

	OT.Identification	OT.Personalisation	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Personalisation	OE.Passive_Auth_Sign	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Terminal	OE.ID_Card-Holder	OE.Legislative_Compliance	OE.CGA_QCert ([7])[83]
P.Terminal																x			
P.ID_Card_PKI													x	x					
P.Terminal_PKI															x				
P.Trustworthy_PKI													x		x				x

Table 10: Security Objective Rationale

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

103 The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the Service Provider) using the TOE's contactless interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the Terminal- and the Chip Authentication. The objective OE.Terminal_Authentication sets a prerequisite up for an effective terminal authentication (its property 'CVCAs must issue their certificates exclusively to the rightful organisations (DV) and DV must issue their certificates exclusively to the rightful equipment (terminals)'). The objective OE.Terminal sets a prerequisite up that no assets will be transferred between the TOE and the Service Provider before the Chip Authentication has successfully been accomplished (in its property 'Their (Service Provider's – remark of the author) terminals must not send assets (e.g. eSign-PIN, DTBS) to the TOE within the PACE session, but first having successfully performed the chip authentication'). The objective OE.ID_Card-Holder ensures that a PACE session can only be established either by the ID_Card holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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

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

106 The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the Service Provider. The security objective OT.Personalisation requires the TOE to limit the write access for the ID_Card to the trustworthy Personalisation Agent (cf. OE.Personalisation). The TOE will protect

the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives OT.Data_Integrity and OT.Data_Authenticity, respectively. The objectives OT.Prot_Phys-Tamper and OT.Prot_Abuse-Func contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A Service Provider operating his terminals according to OE.Terminal and performing the Passive Authentication using the Card Security Object as aimed by OE.Passive_Auth_Sign will be able to effectively verify integrity and authenticity of the data received from the TOE.

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

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

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

110 The OSP **P.Pre-Operational** is enforced by the following security objectives:
OT.Identification is affine to the OSP's property 'traceability before the operational phase';
OT.Personalisation and OE.Personalisation together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents';
OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

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

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

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

114 The OSP **P.Trustworthy_PKI** is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch), by OE.Terminal_Authentication (for CVCA, receiving PKI branch) and by OE.CGA_QCert (see [7]).

115 The rationale related to the security objectives taken over from [7] are exactly the same as given for the respective items of the security policy definitions in sec. 8.4 of [7].

5 Extended Components Definition

116 This protection profile uses components defined as extensions to CC part 2. All these extended components are drawn from [6].

5.1 Definition of the Family FAU_SAS

117 To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

118 The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to:	No other components
Dependencies:	No dependencies
FAU_SAS.1.1	The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

119 To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is

not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

120 The family ‘Generation of random numbers (FCS_RND)’ is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

Component levelling:

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the Family FIA_API

121 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.

122 *Application note 32:* Other families of the class FIA describe only the authentication verification of 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 the 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 entity in the TOE IT environment.

Component levelling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorised user or role*].

5.4 Definition of the Family FMT_LIM

123 The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

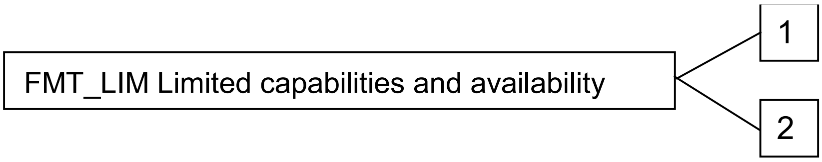
124 The family ‘Limited capabilities and availability (FMT_LIM)’ is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: *Limited capability and availability policy*].

FMT_LIM.2 Limited availability

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited capabilities

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

125 *Application note 33:* The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

5.5 Definition of the Family FPT_EMSEC

126 The family FPT_EMSEC (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [2].

127 The family 'TOE Emanation (FPT_EMSEC)' is specified as follows:

FPT_EMSEC TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

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

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

6 Security Requirements

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

129 The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [1] of the CC. Each of these operations is used in this PP.

130 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~~.

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

132 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as <u>underlined text</u>. 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 *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like <u>*this*</u>.

133 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.
For the sake of a better readability, the iteration operation may also be applied to some single components (being <u>not</u> repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

134 In order to distinguish between the SFRs taken over from the SSCD PP [7] and other SFRs having the same denotation, the author iterated these SFRs by '/SSCD' or '/XXX_SSCD'.

6.1 Security Functional Requirements for the TOE

6.1.1 Overview

135 In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of the PP defined the security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU.1/Rightful_Terminal: Terminal

Security Functional Groups	Security Functional Requirements concerned
	Authentication (EIS, ATT, SGT) – {FDP_ACC.1/Signature-creation_SFP_SSCD, FDP_ACF.1/Signature-creation_SFP_SSCD}
Secure data exchange between the ID_Card and the Service Provider connected	– FTP_ITC.1/CA: trusted channel Supported by: – FCS_COP.1/AES: encryption/decryption – FCS_COP.1/CMAC: MAC generation/verification – FIA_API.1/CA: Chip Identification/Authentication – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PCT) – FIA_UID.1/Rightful_Terminal: Terminal Identification (EIS, ATT, SGT) – FIA_UAU.1/PACE: PACE Authentication (PCT) – FIA_UAU.1/Rightful_Terminal: Terminal Authentication (EIS, ATT, SGT) – FIA_API.1/CA: Chip Identification/Authentication – FIA_UAU.4: single-use of authentication data – FIA_UAU.5: multiple authentication mechanisms – FIA_UAU.6: Re-authentication of Terminal – FIA_AFL.1/eID-PIN_Suspending – FIA_AFL.1/eID-PIN_Blocking: reaction to unsuccessful authentication attempts for establishing PACE communication using *blocking* authentication data – FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using *non-blocking* authentication and authorisation data – FIA_UID.1/SSCD: Identification of ID_Card holder as Signatory (eSign-PIN) – FIA_UIA.1/SSCD: Authentication of ID_Card holder as Signatory (eSign-PIN) – FIA_AFL.1/SSCD: Blocking of the Signatory’s RAD (eSign-PIN)

Security Functional Groups	Security Functional Requirements concerned
	Supported by: – FCS_CKM.1/DH_PACE: PACE authentication (PCT) – FCS_COP.1/SIG_VER: Terminal Authentication (EIS, ATT, SGT) – FCS_CKM.1/DH_CA: Chip Authentication – FCS_CKM.2/DH: Diffie-Hellmann key distribution within PACE and Chip authentication – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_COP.1/SHA: Keys derivation – FCS_RND.1: random numbers generation – FTP_ITC.1/PACE: preventing tracing while establishing Chip Authentication – FMT_SMR.1: security roles definition.
Audit	– FAU_SAS.1 : Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialisation and Pre-personalisation – FMT_MTD.1/INI_DIS: Disabling access to Initialisation and Pre-personalisation Data in the operational phase
Generation of the Signature Key Pair for the eSign application	– FCS_CKM.1/SSCD Supported by: – FCS_CKM.4/SSCD – {FDP_ACC.1/SCD/SVD_Generation_SFP_SSCD, FDP_ACF.1/SCD/SVD_Generation_SFP_SSCD} – {FDP_ACC.1/SVD_Transfer_SFP_SSCD, FDP_ACF.1/SVD_Transfer_SFP_SSCD}
Creation of Digital Signatures by the eSign application	– FCS_COP.1/SSCD
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification/authentication
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT – FDP_RIP.1: enforced memory/storage cleaning – FDP_SDI.2/Persistent_SSCD

Security Functional Groups	Security Functional Requirements concerned
	– FDP_SDI.2/DTBS_SSCD Supported by: – the entire class FMT.

Table 11: Security functional groups vs. SFRs

136 The following table provides an overview of the keys and certificates used for enforcing the security policy defined in the current PP:

Name	Data
Receiving PKI branch	
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF-data to verify the Document Verifier Certificates.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [11] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) an identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Terminal Certificate (C_T)	The Terminal Certificate (C_T) is issued by the Document Verifier. It contains (i) the Terminal Public Key (PK_{PCD}) as authentication reference data, (ii) the coded access control rights of the terminal (EIS, ATT, SGT), the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Issuing PKI branch	
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the ID_Card Issuer signs the Document Signer Public Key Certificate (C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA}) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK_{CSCA}). The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [8], 5.1.1.

Name	Data
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Card Security Object (SO_C) of the ID_Card with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS}).
Chip Authentication Public Key (PK_{PICC})	PK_{PICC} is stored in an EF on the ID_Card and used by the terminal for the Chip Authentication. Its authenticity is verified by the terminal in the context of the Passive Authentication (verification of SO_C).
Chip Authentication Private Key (SK_{PICC})	The Chip Authentication Key Pair {SK_{PICC}, PK_{PICC}} is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 (ver. 1.11, BSI, 2009), cf. [11], table. A.2. SK_{PICC} is used by the TOE to authenticate itself as authentic ID_Card.
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal (PCT) as result of the PACE Protocol, see [11], sec. A.3, F.2.2, A.2.3.2.
Chip Authentication Session Keys (CA-K_{MAC}, CA-K_{Enc})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) agreed between the TOE and a terminal (EIS, ATT, SGT) as result of the Chip Authentication Protocol, see [11], sec. A.4, F.2.2, A.2.3.2.
Restricted Identification keys	
Restricted Identification Key Pair {SK_{ID}, PK_{ID}}	Static Diffie-Hellman key pair, whereby the related private key SK_{ID} is stored in the TOE and used for generation of the sector-specific chip-identifier I_{ID}^{Sector} (pseudo-anonymisation), see [11], sec. 4.1.2, 4.1.3.1, 4.5.1. This key represents user data (Table 2, object no. 1) within the current security policy, cf. Table 2, object #1. The belonging public key PK_{ID} is used for a revocation request and should not be stored in the TOE, see [11], sec. 4.1.2, 4.1.3.1, 4.5.3. For Restricted Identification please also refer to the *Application note 6*.
Signature keys	
Signature Creation Key Pair {SCD, SVD}	Signature Creation Data (SCD) is represented by a private cryptographic key being used by the ID_Card holder (signatory) to create an electronic signature. This key represents user data (Table 2, object no. 1). Signature Verification Data (SVD) is represented by a public cryptographic key corresponding with SCD and being used for the purpose of verifying an electronic signature.

Name	Data
	Properties of this key pair shall fulfil the relevant requirements stated in [15].

Table 12: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

137 **FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman for PACE session keys**

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/ DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [13]*][84] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [11], Appendix A.3 [85].

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

138 *Application note 34:* The TOE generates a shared secret value with the terminal during the PACE protocol, see [11], sec. 4.2 and A.3. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [17]) or on the ECDH compliant to TR-03111 [13] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [11], Appendix A.3 and [13] for details). The shared secret value is used to derive the AES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [11], F.2.2 and A.2.3.2 for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

139 **FCS_CKM.1/DH_CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

84 [*assignment: cryptographic key generation algorithm*]

85 [assignment: *list of standards*]

	FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.2/DH.
	FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ DH_CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [13]*][86] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [11], Annex A.4 [87].

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

140 *Application note 35:* The TOE generates a shared secret value with the terminal during the CA Protocol, see [11], sec. 4.3 and A.4. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [17]) or on the ECDH compliant to TR-03111 [13] (i.e. an elliptic curve cryptography algorithm, cf. [11], Appendix A.4 and [13] for details). The shared secret value is used to derive the AES session keys for message encryption and message authentication (CA-K_{MAC}, CA-K_{Enc}) according to the [11], F.2.2 and A.2.3.2 for the TSF required by FCS_COP.1/AES and FCS_COP.1/CMAC.

141 **FCS_CKM.2/DH** **Cryptographic key distribution – Diffie-Hellman**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]: fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA FCS_CKM.4: fulfilled by FCS_CKM.4
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the list below[88] that meets the following: a) PACE: as specified in [11], sec. 4.2 and A.3; b) CA: as specified in [11], sec. 4.3 (version 2) and A.4[89].

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

142 **FCS_CKM.4** **Cryptographic key destruction – Session keys**

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

86 [*assignment: cryptographic key generation algorithm*]

87 [assignment: *list of standards*]

88 [assignment: *cryptographic key distribution method*]

89 [assignment: *list of standards*]

	FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

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

143 *Application note 36:* The TOE shall destroy the PACE session keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the CA session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

6.1.2.2 Cryptographic operation (FCS_COP.1)

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: not fulfilled, but **justified** A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here. FCS_CKM.4 Cryptographic key destruction: not fulfilled, but **justified** A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.
FCS_COP.1.1/ SHA	The TSF shall perform <u>hashing</u> [90] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes <u>none</u> [91] that meet the following: <u>FIPS 180-2 [19]</u>[92].

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

90 [assignment: *list of cryptographic operations*]

91 [assignment: *cryptographic key sizes*]

92 [assignment: *list of standards*]

145 *Application note 37:* For compressing (hashing) an ephemeral public key for DH (PACE[93] and CA[94]), the hash function SHA-1 shall be used ([11], table A.2).
The TOE shall implement hash functions either SHA-1 or SHA-224 or SHA-256 for the Terminal Authentication Protocol (cf. [11], tables A.12 and A.13).
Within the normative Appendix A of [11], section A.2.3 'Key Derivation Function', [11] states that the hash function SHA-1 shall be used for deriving 128-bit AES keys, whereas SHA-256 – for deriving 192-bit and 256-bit AES keys.

146 **FCS_COP.1/SIG_VER Cryptographic operation – Signature verification**

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: not fulfilled, but **justified** The root key PK_{CVCA} used for verifying C_{DV} is stored in the TOE during its personalisation (in the card issuing life phase)[95]. Since importing the respective certificates (C_T, C_{DV}) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3 below), the 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, needn't to be destroyed.
FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification [96] 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*].

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

147 A*pplication note 38:* The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal Authentication Protocol (cf. [11], Appendix A.6.3, A.6.4 and D.3 for details). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal generated a digital signature for the TOE challenge, see [11], sec. 4.4. The related static public keys (PK_{PCD}, PK_{DV}) are imported within the respective certificates (C_T, C_{DV}) during the TA

93 ID_{PICC} ≡ Comp(ephem-PK_{PICC}-PACE) in [11], sec. 4.4; the public key compression function is defined in table A.2 of [11].

94 Comp(ephem-PK_{PCD}-TA) in [11], sec. 4.3.1.2; the public key compression function is defined in table A.2 of [11].

95 as already mentioned, operational use of the TOE is explicitly in focus of the current PP

96 [assignment: *list of cryptographic operations*]

and are extracted by the TOE using PK_{CVCA} as the root key stored in the TOE during its personalisation (see P.Terminal_PKI).

148 **FCS_COP.1/AES** **Cryptographic operation – Encryption / Decryption AES**

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

FCS_COP.1.1/AES The TSF shall perform secure messaging – encryption and decryption [97] in accordance with a specified cryptographic algorithm AES in CBC mode [98] and cryptographic key sizes [selection: *128, 192, 256*] bit [99] that meet the following: FIPS 197 [16] and [11] Appendix F.2.2[100].

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

149 *Application note 39:* 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 according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}) or the Chip Authentication Protocol according to the FCS_CKM.1/DH_CA (CA-K_{Enc}). Note that in accordance with [11] Appendix F.2.1 and A.2.3.1 the (two-key) Triple-DES could be used in CBC mode for secure messaging. Due to the fact that the (two-key) Triple-DES is not recommended any more (cf. [12], sec. 1.3), Triple-DES in any mode is no longer applicable within this PP.

150 **FCS_COP.1/CMAC** **Cryptographic operation – CMAC**

Hierarchical to: No other components.

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

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

97 [assignment: *list of cryptographic operations*]

98 [assignment: *cryptographic algorithm*]

99 [assignment: *cryptographic key sizes*]

100 [assignment: *list of standards*]

FCS_COP.1.1/ CMAC — The TSF shall perform secure messaging – message authentication code [101] in accordance with a specified cryptographic algorithm CMAC [102] and cryptographic key sizes [selection: *128, 192, 256*] bit [103] that meet the following: 'The CMAC Mode for Authentication, NIST Special Publication 800-38B' [18] and [11] Appendix F.2.2[104].

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

151 *Application note 40*: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}) or the Chip Authentication Protocol according to the FCS_CKM.1/DH_CA (CA-K_{MAC}). Note that in accordance with [11] Appendix F.2.1 and A.2.3.1 the (two-key) Triple-DES could be used in Retail mode for secure messaging. Due to the fact that the (two-key) Triple-DES is not recommended any more (cf. [12], sec. 1.3), Triple-DES in any mode is no longer applicable within this PP.

6.1.2.3 Random Number Generation (FCS_RND.1)

152 **FCS_RND.1** **Quality metric for random numbers**

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

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

153 *Application note 41*: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols (PACE, CA and TA) as required by FIA_UAU.4.

154 The current PP also includes all SFRs of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational. For the functional class FCS, there are the following components:

SFR identifier	Comments

101 [assignment: *list of cryptographic operations*]

102 [assignment: *cryptographic algorithm*]

103 [assignment: *cryptographic key sizes*]

104 [assignment: *list of standards*]

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

6.1.3 Class FIA Identification and Authentication

155 For the sake of better readability, Table 13 provides an overview of the authentication mechanisms used:

Name	SFR for the TOE	Comments
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5 FIA_AFL.1/eID-PIN_Suspending FIA_AFL.1/eID-PIN_Blocking FIA_AFL.1/PACE	as required by FCS_CKM.1/DH_PACE
Terminal Authentication Protocol	FIA_UAU.1/Rightful_Terminal FIA_UAU.5	as required by FCS_COP.1/SIG_VER
Chip Authentication Protocol	FIA_API.1/CA, FIA_UAU.5, FIA_UAU.6	as required by FCS_CKM.1/DH_CA
eSign-PIN	FIA_UAU.1/SSCD	inherited from [7]

Table 13: Overview of authentication SFRs

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

Hierarchical to: No other components.

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

FIA_AFL.1.1 The TSF shall detect when [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 eID-PIN as the shared password for PACE[105].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[106], the TSF shall suspend the reference value of eID-PIN according to [11], sec. 3.3.2[107].

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

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

Hierarchical to: No other components.

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

FIA_AFL.1.1 The TSF shall detect when [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 suspended[108] eID-PIN as the shared password for PACE[109].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[110], the TSF shall block the reference value of eID-PIN according to [11], sec. 3.3.2[111].

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

158 *Application note 42:* According to [11], sec. 3.3.2, a *suspending* current value of the retry counter for eID-PIN shall be RC = 1, the *blocking* current value of the retry counter for eID-PIN shall be RC = 0; no initial value of RC is defined in [11]. The assignment shall be consistent with the implemented authentication mechanism and resistant against attacks with high attack potential.

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

Hierarchical to: No other components.

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

FIA_AFL.1.1 The TSF shall detect when 1[112] unsuccessful authentication attempts occurs related to authentication attempts using CAN, MRZ, eID-PUK as shared passwords for PACE[113].

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

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

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

[108] as required by FIA_AFL.1/eID-PIN_Suspending

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

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

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[114], the TSF shall [assignment: *list of actions*].

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

160 *Application Note 43*: The open assignment operation shall be performing according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (CAN, MRZ, eID-PUK) or for an arbitrary subset of them or may also separately be defined for each datum in question.
Since all non-blocking authorisation and authentication data (CAN, MRZ and eID-PUK) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[115], the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack[116] requiring an attack potential beyond high, so that the threat T.ID_Card_Tracing can be averted in the frame of the security policy of the current PP.
One of some opportunities for performing this operation might be 'consecutively increase the reaction time of the TOE to the next authentication attempt using CAN, MRZ, eID-PUK'.

161 *Application Note 44*: Please note that since guessing CAN, MRZ and eID-PUK requires an attack potential beyond high according to the current PP, monitoring the static PK_{PICC} and SO_C in the context of the chip authentication will also fail (due to FTP_ITC.1/PACE), so that it is not essential, whether PK_{PICC} and SO_C 'ID_Card-generation / batch' or 'ID_Card-individual' data are.

162 **FIA_API.1/CA** **Authentication Proof of Identity**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide the Chip Authentication Protocol according to [11], sec. 4.3, Version 2 [117] to prove the identity of the TOE [118].

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

163 *Application note 45:* The Chip Authentication shall be triggered by a rightful terminal immediately after the successful Terminal Authentication (as required FIA_UAU.1/Rightful_Terminal) using, amongst other, Comp(ephem-PK_{PCD}-TA)[119] from the

---

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

113 [assignment: *list of authentication events*]

114 [selection: *met ,surpassed*]

115 ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.

116 guessing CAN or MRZ or eID-PUK, see T.Skimming above

117 [assignment: *authentication mechanism*]

118 [assignment: *authorised user or role*]

119 Comp() is public key compression function. It is defined in [11], table A.2 as SHA-1 (for Diffie-Hellmann)

accomplished TA. The terminal verifies genuineness of the ID_Card by verifying the authentication token T_{PICC} calculated by the ID_Card using ephem-PK_{PCD}-TA and CA-K_{MAC}, (and, hence, finally making evident possessing the Chip Authentication Key (SK_{PICC})).
The Passive Authentication making evident authenticity of the PK_{PICC} by verifying the Card Security Object (SO_C) up to CSCA shall be triggered by the rightful terminal immediately after the successful Terminal Authentication before the Chip Authentication[120] and is considered to be part of the CA protocol within this PP (see also P.Terminal).
Please note that this SFR does not require authentication of any TOE's user, but providing evidence enabling an external entity (the terminal connected) to prove the TOE's identity.
If the Chip Authentication was successfully performed, Secure Messaging is restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc}), cf. FTP_ITC.1/CA. Otherwise, Secure Messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

164 **FIA_UID.1/PACE** **Timing of identification**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE Protocol according to [11], sec. 4.2[121] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

165 *Application note 46:* User identified after a successfully performed PACE protocol is a PACE terminal (PCT). In case eID-PIN or eID-PUK were used for PACE, it is the ID_Card holder using PCT. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. in case CAN or MRZ were used for PACE, it is either the ID_Card holder itself or an authorised other person or device.

166 **FIA_UID.1/Rightful_Terminal** **Timing of identification**

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

[120] cf. [11], sec. 3.4

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

FIA_UID.1.1 The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE protocol according to [11], sec. 4.2,
3. carrying out the Terminal Authentication Protocol according to [11], sec. 4.4, Version 2[122]

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

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

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

167 *Application note 47:* The user identified after a successfully performed TA protocol is a rightful terminal, i.e. either EIS or ATT or SGT.

168 *Application note 48:* In the life phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.
Please note that a Personalisation Agent acts on behalf of the ID_Card Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal (e.g. ATT) proves the respective Terminal Authorisation Level.

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

Hierarchical to: No other components.

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

FIA_UAU.1.1 The TSF shall allow

1. establishing a communication channel,
2. carrying out the PACE Protocol according to [11], sec. 4.2[123],[124]

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

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

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

---

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

123 ID_Card identifies itself within the PACE protocol by selection of the authentication key ephem-PK_{PICC}-PACE

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

170 *Application note 49:* The user authenticated after a successfully performed PACE protocol is a PACE terminal (PCT). In case eID-PIN or eID-PUK were used for PACE, it is the ID_Card holder using PCT. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. in case CAN or MRZ were used for PACE, it is either the ID_Card holder itself or an authorised other person or device.
If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

171 **FIA_UAU.1/Rightful_Terminal Timing of authentication**

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/Rightful_Terminal
FIA_UAU.1.1	The TSF shall allow 1. establishing a communication channel, 2. carrying out the PACE protocol according to [11], sec. 4.2, 3. carrying out the Terminal Authentication Protocol according to [11], sec. 4.4, Version 2[125,126] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

172 *Application note 50:* The user authenticated after a successfully performed TA protocol is a Service Provider represented by a rightful terminal, i.e. either EIS or ATT or SGT. The authenticated terminal will immediately perform the Chip Authentication (Version 2) as required by FIA_API.1/CA using, amongst other, Comp(ephem-PK_{PCD}-TA) from the accomplished TA. Please note that the Passive Authentication is considered to be part of the CA protocol within this PP.

173 **FIA_UAU.4 Single-use authentication of the Terminals by the TOE**

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

[125] ID_Card identifies itself within the TA protocol by using the identifier $ID_{PICC} \equiv$ Comp(ephem-PK_{PICC}-PACE).

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

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

1. PACE Protocol according to [11], sec. 4.2,
2. Terminal Authentication Protocol according to [11], sec. 4.4, Version 2.[127]

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

174 *Application note 51:* For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed (the current PP supports the key derivation function based on AES; see [11], sec. A.3.3 and A.2.3). For the TA protocol, the TOE randomly selects a nonce r_{PICC} of 64 bits length, see [11], sec. B.3 and B.11.6.

175 **FIA_UAU.5** **Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

the General Authentication Procedure as the sequence

1. PACE Protocol according to [11], sec. 4.2,
2. Terminal Authentication Protocol according to [11], sec. 4.4, Version 2,
3. Chip Authentication Protocol according to [11], sec. 4.3, Version 2°[128],

and

4. Secure messaging in encrypt-then-authenticate mode according to [11], Appendix F [129]

to support user authentication.

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

[128] the Passive Authentication is considered to be part of the Chip Authentication (CA) Protocol within this PP.

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

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

1. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol, only if (i) the terminal presents its static public key[130] being successfully verifiable up to CVCA and (ii) the terminal uses the PICC identifier[131] calculated during and the secure messaging established by the current PACE authentication.
2. Having successfully run the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the Chip Authentication Protocol.[132]

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

176 *Application note 52:* Please note that Chip Authentication Protocol does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the TOE's identity.

177 **FIA_UAU.6 Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the rightful terminal. [133]

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

178 *Application note 53:* The PACE and the Chip Authentication protocols specified in [11] start secure messaging used for all commands exchanged after successful PACE authentication and CA. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CMAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal. For the Terminal Authentication, the current secure messaging session is bounded on Comp(ephem-PK_{PCD}-TA).

130 PK_{PCD}

131 $ID_{PICC} \equiv$ Comp(ephem-PK_{PICC}-PACE)

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

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

179 The current PP also includes all SFRs of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational. For the functional class FIA, there are the following components, whereby the component FIA_UAU.1/SSCD is explicitly re-defined (supplemented) in the current PP:

180 **FIA_UAU.1/SSCD** **Timing of authentication**

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/SSCD, cf. [7]
FIA_UAU.1.1	The TSF shall allow 1. self test according to FPT_TST.1, 2. identification of the user by means of TSF required by FIA_UID.1/SSCD in [7], 3. establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/CA[134], 4. establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/CA[135], 5. [assignment: *list of additional TSF-mediated actions*][136] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

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

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

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

[136] [assignment: *list of TSF mediated actions*]

6.1.4 Class FDP User Data Protection

181 **FDP_ACC.1/TRM** **Subset access control – Terminal Access**

Hierarchical to: No other components.

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

FDP_ACC.1.1 The TSF shall enforce the Terminal Access Control SFP [137] on terminals gaining write, read, modification and usage access to the User Data stored in the ID_Card [138].

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

182 **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 initialisation: not fulfilled, but **justified**

The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

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

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

FDP_ACF.1.1 The TSF shall enforce the Terminal Access Control SFP[139] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. PACE Terminal (PCT),
   c. Rightful Terminal (EIS, ATT, SGT);
2. Objects:
   User Data stored in the TOE;
3. Security attributes:
   a. Authentication status of terminals,
   b. Terminal Authorisation Level,
   c. CA authentication status,
   d. Authentication status of the ID_Card holder as Signatory (if the *eSign* is operational) [140].

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

1. a successfully authenticated Extended Inspection System (EIS) is allowed to read User Data according to [11], sec. C.4.1.1 after a successful CA as required by FIA_API.1/CA.
2. a successfully authenticated Authentication Terminal (ATT) is allowed to read, modify and write User Data as well as to generate signature key pair(s) within the eSign application (SCD/SVD[141]) according to [11], sec. C.4.1.2 after a successful CA as required by FIA_API.1/CA.
3. a successfully authenticated Signature Terminal (SGT) is allowed to use the private signature key within the eSign application (SCD, if the *eSign* is operational) for generating digital signatures according to [11], sec. C.4.1.3 after a successful CA as required by FIA_API.1/CA and a successful authentication of the ID_Card holder as Signatory as required by FIA_UAU.1/SSCD. [142]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[143].

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

1. Any terminal (including PCT) being not authenticated as a rightful terminal (i.e. as either EIS or ATT or SGT) is not allowed to read, to write, to modify, to use any User Data stored on the ID_Card.
2. Nobody is allowed to read 'TOE immanent secret cryptographic

---

139 [assignment: *access control SFP*]

140 [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*]

141 as required by FCS_CKM.1/SSCD

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

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

keys' stored on the ID_Card.

3 Nobody is allowed to read 'secret ID_Card holder authentication data' stored on the ID_Card.

4. Nobody is allowed to read the private Restricted Identification (SK_{ID}) key stored on the ID_Card.

5. Nobody is allowed to read the private signature key(s) within the eSign application (SCD; if the *eSign* is operational)[144].

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

183 *Application note 54*: The relative certificate holder (Service Provider) authorisation is encoded in the Card Verifiable Certificate of the terminals being operated by the Service Provider. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Terminal Certificate (cf. FMT_MTD.3). The Terminal Authorisation Level is the intersection of the Certificate Holder Authorisation in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Terminal Certificate in a valid certificate chain. It is technically based on Certificate Holder Authorization Template (CHAT), see [11], C.1.5. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ID_Card holder's restricting input at the terminal. This final CHAT reflects the *effective authorisation level*, see [11], C.4.2 and is then sent to the TOE by the command 'MSE:Set AT' within the Terminal Authentication (B.3 und B.11.1 of [11]).

184 *Application note 55*: Please note that the General Authentication Procedure as required by FIA_UAU.5 is mandatory for all the applications residing on the TOE, see [11], sec. 3.4; cf. also table E.1. Concerning table 1.2 of [11], the current PP supports only 'EAC version 2', whereby EAC shall be mandatory for all user data (DG1 – DG16) of the *ePassport*.
Please note that the Card Security Object (SO_C) does not belong to the user data, but to the TSF-data. The Card Security Object can be read out by the PCT, see [11], A.1.2 and table A.1 for EF.CardSecurity.

185 *Application note 56*: Please note that this functional requirement also covers the ability to activate the *eSign* application using the ATT with an appropriate Terminal Authorisation Level, see [11], sec. C.4.1.2, and acting on behalf of the CSP and upon an application by the ID_Card holder.

186 *Application note 57*: Please note that the control on the user data transmitted between the TOE and the rightful terminal is addressed by FTP_ITC.1/CA.

187 **FDP_RIP.1** **Subset residual information protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

1. the Chip Authentication Private Key (SK_{PICC}),
2. the secret ID_Card holder authentication data eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational),
3. the session keys (PACE-K_{MAC}, PACE-K_{Enc}), (CA-K_{MAC}, CA-K_{Enc}),
4. the private Restricted Identification key SK_{ID},
5. the private signature key of the ID_Card holder (SCD; if the *eSign* is operational),
5. [assignment: *list of (further) objects*].

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

188 *Application note 58*: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMSEC.

189 *Application note 59*: Please note that FDP_RIP.1 also contributes to achievement of OT.Sigy_SigF (eSign-PIN) and OT.SCD_Secrecy (SCD) from [7].

190 The current PP also includes all SFRs of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational. For the functional class FDP, there are the following components:

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

SFR identifier	Comments
	– eSign
FDP_SDI.2/DTBS_SSCD	concerns the following application(s): – eSign

6.1.5 Class FTP Trusted Path/Channels

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **PACE terminal (PCT) after PACE** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ~~another trusted IT product~~ **the PCT**[145] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the PCT after PACE. [146]

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

192 *Application note 60*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while establishing Chip Authentication; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/AES and FCS_COP.1/CMAC.
The PACE secure messaging session is immediately superseded by a CA secure messaging session after successful Chip Authentication as required by FTP_ITC.1/CA.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE and FIA_AFL.1/eID-PIN_Blocking.

193 **FTP_ITC.1/CA** **Inter-TSF trusted channel after CA**

---

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

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **rightful terminal (EIS, ATT, SGT) after Chip Authentication** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit ~~another trusted IT product~~ **the rightful terminal (EIS, ATT, SGT)**[147] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Service Provider represented by the rightful terminal after Chip Authentication. [148]

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

194 *Application note 61*: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE), the TA protocol (FIA_UAU.1/Rightful_Terminal) and the CA protocol (FIA_API.1/CA). If the Chip Authentication was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc})[149]: 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/AES and FCS_COP.1/CMAC.

195 *Application note 62*: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

196 *Application note 63*: The requirement FTP_ITC.1/CA also covers a secure transport of (i) SVD[150] from the TOE to CGA[151] as well as of (ii) VAD[152] from HID[153] and of (iii) DTBS[154] from SCA[153] to the TOE. It also covers TOE's capability to generate and to provide CGA with evidence that can be used as a guarantee of the validity of SVD. The current SFR reflects the main additional feature concerning the eSign application comparing to [7].

6.1.6 Class FAU Security Audit

197 **FAU_SAS.1** **Audit storage**

---

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

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

149 otherwise, secure messaging is continued using the previously established session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

150 integrity is to secure

151 the authenticated terminal is ATT with bits 7 (install qualified certificate) or/and 6 (install certificate) set to 1, cf. [11], sec. C.4.1.2.

152 confidentiality is to secure

153 the authenticated terminal is SGT

154 integrity is to secure

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[155] with the capability to store the Initialisation and Pre-Personalisation Data [156] in the audit records.

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

198 *Application note 64*: The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the ID_Card manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the ID_Card (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.7 Class FMT Security Management

199 The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements on the management of the TSF data.

200 **FMT_SMF.1** **Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialisation,
2. Personalisation,
3. Configuration,
4. Resume and unblock the eID-PIN[157],
5. Activate and deactivate the eID-PIN. [158]

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

201 **FMT_SMR.1** **Security roles**

Hierarchical to: No other components.

155 [assignment: *authorised users*]

156 [assignment: *list of audit information*]

157 unblocking eSign-PIN is managed by FMT_SMF.1/SSCD

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

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE, FIA_UID.1/Rightful_Terminal
see also the *Application note 65* below.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalisation Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. Terminal,
6. PACE Terminal (PCT),
7. (Extended) Inspection System (EIS),
8. Authentication Terminal (ATT),
9. Signature Terminal (SGT),
10. ID_Card holder. [159]

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

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

202 *Application note 65*: For explanation on the role Manufacturer please refer to the *Application note 64*; on the role Personalisation Agent – to the *Application note 48*. The role Terminal is the default role for any terminal being recognised by the TOE as neither PCT nor EIS nor ATT nor SGT ('Terminal' is used by the ID_Card presenter). The roles CVCA, DV, EIS, ATT[160] and SGT are recognised by analysing the current Terminal Certificate C_T, cf. [11], C.4 (FIA_UAU.1/Rightful_Terminal). The TOE recognises the ID_Card holder by using PCT upon input eID-PIN or eID-PUK (FIA_UAU.1/PACE) as well as – in the context of the eSign application – by using SGT upon input eSign-PIN (FIA_UAU.1/SSCD).

203 The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

204 **FMT_LIM.1** **Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2

159 [assignment: *the authorised identified roles*]

160 ATT plays a special role 'CGA' for the *eSign* application, if bits 7 (install qualified certificate) or/and 6 (install certificate) are set to 1 within the effective terminal authorisation level, cf. [11], sec. C.4.1.2; an ATT with such an terminal authorisation level is authorised by the related CSP to act as CGA on its behalf.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced:
Deploying test features after TOE delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[161]

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

205 **FMT_LIM.2** **Limited availability**

Hierarchical to: No other components.

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

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:
Deploying test features after TOE delivery do not allow

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. embedded software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks. [162]

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

206 **FMT_MTD.1/INI_ENA** **Management of TSF data – Writing Initialisation and Pre-personalisation Data**

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to write [163] the Initialisation Data and Pre-personalisation Data[164] to the Manufacturer [165].

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

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

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

207 **FMT_MTD.1/INI_DIS** **Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to read out and to use [166] the Initialisation Data [167] to the Personalisation Agent [168].

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

208 *Application note 66:* The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life phase 'issuing' to the life phase 'operational use'. Please also refer to the *Application note 48*.

209 **FMT_MTD.1/CVCA_INI** **Management of TSF data – Initialisation 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

---

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

164 [assignment: *list of TSF data*]

165 [assignment: *the authorised identified roles*]

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

167 [assignment: *list of TSF data*]

168 [assignment: *the authorised identified roles*]

FMT_MTD.1.1 The TSF shall restrict the ability to write [169] the

1. initial Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the initial Country Verifying Certification Authority Certificate (C_{CVCA}) as required in [11], sec. A.6.2.3,
3. initial Current Date,
4. [assignment: *list of TSF data*]

to [assignment: *the authorised identified roles*].

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

210 *Application note 67:* The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the manufacturing phase or by the Personalisation Agent in the issuing phase (cf. [11], sec. 2.2.5). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The metadata of the initial Country Verifying Certification Authority Certificate and the initial Current Date are needed for verification of the certificates and the calculation of the Terminal Authorisation Level. Please note that only a *subset* of the metadata must be stored in the TOE, see [11], sec. A.6.2.3; storing of further certificate's content is optional.

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

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to update [170] the

1. Country Verifying Certification Authority Public Key (PK_{CVCA}),
2. metadata of the Country Verifying Certification Authority Certificate (C_{CVCA}) as required in [11], sec. A.6.2.3,
3. [assignment: *list of TSF data*]

to Country Verifying Certification Authority [171].

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

212 *Application note 68:* The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key and the related metadata be means of the CVCA Link-Certificates (cf. [11], sec. 2.2). The TOE updates its internal trust-point, if a valid CVCA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [11], sec. 2.2.3 and 2.2.5).

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

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

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

171 [assignment: *the authorised identified roles*]

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to modify [172] the Current Date[173] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Rightful Terminal (EIS, ATT or SGT) possessing an Accurate Terminal Certificate[174].

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

214 *Application note 69*: The authorised roles are identified in their certificates (cf. [11], sec. 2.2.5 and C.4) and authorised by validation of the certificate chain up to CVCA (cf. FMT_MTD.3). The authorised role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal within the Terminal Authentication (cf. [11], A.6.2.3, B.11.1, C.1.3, C.1.5, D.2 for details).

215 **FMT_MTD.1/PA_UPD** **Management of TSF data – Personalisation Agent**

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to write [175] the Card Security Object (SO_C)[176] to the Personalisation Agent. [177]

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

216 *Application note 70*: Please refer to the *Application note 48*.

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

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

173 [assignment: *list of TSF data*]

174 [assignment: *the authorised identified roles*]

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

176 [assignment: *list of TSF data*]

177 [assignment: *the authorised identified roles*]

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *create, load*] [178] the Chip Authentication Private Key (SK_{PICC})[179] to [assignment: *the authorised identified roles*].

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

218 *Application note 71:* 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 is generated securely outside the TOE and written into the TOE memory. The verb 'create' means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer might include an appropriate instantiation of the component FCS_CKM.1 as SFR for this key generation.

219 **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

FMT_MTD.1.1 The TSF shall restrict the ability to read [180] the Chip Authentication Private Key (SK_{PICC}) [181] to none. [182]

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

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

Hierarchical to: No other components.

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

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to resume [183] the suspended eID-PIN [184] to the ID_Card holder. [185]

---

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

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

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

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

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

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

221 *Application note 72:* The resuming procedure is a two-step one, subsequently using PACE with CAN and PACE with eID-PIN. It must be implemented according to [11], sec. 3.5.1 and is relevant for the status as required by FIA_AFL.1/eID-PIN_Suspending. The ID_Card holder is authenticated as required by FIA_UAU.1/PACE using the eID-PIN as the shared password.

222 **FMT_MTD.1/eID-PIN_Unblock Management of TSF data – Unblocking/Changing eID-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

FMT_MTD.1.1 The TSF shall restrict the ability to unblock and change [186] the blocked eID-PIN [187] to

1. the ID_Card holder,
2. the Authentication Terminal (ATT) with the Terminal Authorisation Level for eID-PIN management. [188]

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

223 *Application note 73:* The unblocking procedure must be implemented according to [11], sec. 3.5.1, 3.5.2 and is relevant for the status as required by FIA_AFL.1/eID-PIN_Blocking. It can be triggered by either (i) the ID_Card holder being authenticated as required by FIA_UAU.1/PACE using the eID-PUK as the shared password or (ii) the ATT (FIA_UAU.1/Rightful_Terminal) proved a Terminal Authorisation Level being sufficient for eID-PIN management (FDP_ACF.1/TRM).

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

Hierarchical to: No other components.

---

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

184 [assignment: *list of TSF data*]

185 [assignment: *the authorised identified roles*]

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

187 [assignment: *list of TSF data*]

188 [assignment: *the authorised 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

FMT_MTD.1.1 The TSF shall restrict the ability to activate and deactivate [189] the eID-PIN [190] to the Authentication Terminal (ATT) with the Terminal Authorisation Level for eID-PIN management. [191]

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

225 *Application note 74:* The activating/deactivating procedures must be implemented according to [11], sec. 3.5.2. It can be triggered by the ATT (FIA_UAU.1/Rightful_Terminal) proved a Terminal Authorisation Level being sufficient for eID-PIN management (FDP_ACF.1/TRM).

226 **FMT_MTD.3** **Secure TSF data**

Hierarchical to: No other components.

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

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol and the Terminal Access Control SFP.[192]

Refinement: The certificate chain is valid if and only if

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

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

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

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

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

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

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

[192] [assignment: list of TSF data]

The intersection of the Certificate Holder Authorisations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorisation Level[193] of a successfully authenticated Service Provider (represented by a rightful terminal).

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

227 *Application note 75:* The Terminal Authentication is used as required by FIA_UAU.1/Rightful_Terminal and FIA_UAU.5. The Terminal Authorisation Level[193] derived from the C_{CVCA}, C_{DV} and C_T is used as TSF-data for the access control required by FDP_ACF.1/TRM.

228 The current PP also includes all SFRs of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational. For the functional class FMT, there are the following components:

SFR identifier	Comments
FMT_SMR.1/SSCD	concerns the following application(s): – eSign
FMT_SMF.1/SSCD	concerns the following application(s): – eSign
FMT_MOF.1/SSCD	concerns the following application(s): – eSign
FMT_MSA.1/Admin_SSCD	concerns the following application(s): – eSign
FMT_MSA.1/Signatory_SSCD	concerns the following application(s): – eSign
FMT_MSA.2/SSCD	concerns the following application(s): – eSign
FMT_MSA.3/SSCD	concerns the following application(s): – eSign
FMT_MSA.4/SSCD	concerns the following application(s): – eSign
FMT_MTD.1/Admin_SSCD	concerns the following application(s): – eSign
FMT_MTD.1/Signatory_SSCD	concerns the following application(s):

193 this certificate-calculated Terminal Authorisation Level can additionally be restricted by ID_Card holder at the terminal, s. [11], sec. C.4.2. It is based on Certificate Holder Authorization Template (CHAT), see [11], C.1.5. A CHAT is calculated as an AND-operation from the certificate chain of the terminal and the ID_Card holder's restricting input at the terminal. This final CHAT reflects the *effective authorisation level*, see [11], C.4.2 and is then sent to the TOE by the command 'MSE:Set AT' within the Terminal Authentication (B.3 und B.11.1 of [11]).

SFR identifier	Comments
	– eSign eSign-PIN can be unblocked using the card-global eID-PUK and may also be unblocked using an eSign-specific eSign-PUK, if any.

6.1.8 Class FPT Protection of the Security Functions

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

230 **FPT_EMSEC.1** **TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. the Chip Authentication Private Key (SK_{PICC}),
2. the eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational),
3. [assignment: *list of types of (further) TSF data*]

and

4. the private Restricted Identification key SK_{ID},
5. the private signature key of the ID_Card holder (SCD; if the *eSign* is operational),
6. [assignment: *list of types of (further) user data*].

FPT_EMSEC.1.2 The TSF shall ensure any users [194] are unable to use the following interface ID_Card's contactless interface and circuit contacts [195] to gain access to

[194] [assignment: *type of users*]

[195] [assignment: *type of connection*]

1. the Chip Authentication Private Key (SK_{PICC}),
2. the eID-PIN, eID-PUK, eSign-PIN (RAD; if the *eSign* is operational),
3. [assignment: *list of types of (further) TSF data*]

and

4. the private Restricted Identification key SK_{ID},
5. the private signature key of the ID_Card holder (SCD; if the *eSign* is operational),
6. [assignment: *list of types of (further) user data*].

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

231 *Application note 76*: 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 or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The ID_Card's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

232 The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

233 **FPT_FLS.1** **Failure with preservation of secure state**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. [assignment: *list of types of (further) failures in the TSF*].

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

234 **FPT_TST.1** **TSF testing**

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

FPT_TST.1.1	The TSF shall run a suite of self tests [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [*assignment: conditions under which self test should occur]*] to demonstrate the correct operation of the TSF[196].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[197].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

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

235 *Application note 77*: If the ID_Card's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

236 **FPT_PHP.3** **Resistance to physical attack**

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing [198] to the TSF [199] by responding automatically such that the SFRs are always enforced.

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

237 *Application note 78*: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

---

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

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

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

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

238 The current PP also includes all SFRs of the SSCD PP [7]. These items are applicable, if the *eSign* application is operational. For the functional class FPT, there are the following components:

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

6.2 Security Assurance Requirements for the TOE

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

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

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.Identification	OT.Personalisation	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.SCD/SVD_Gen [7][200]	OT.Sigy_SigF [7][200]
FCS_CKM.1/DH_PACE			x	x	x								
FCS_CKM.1/DH_CA			x	x	x								
FCS_CKM.2/DH			x	x	x		x						
FCS_CKM.4			x	x	x								
FCS_COP.1/SHA			x	x	x		x						
FCS_COP.1/SIG_VER			x	x	x								
FCS_COP.1/AES					x								
FCS_COP.1/CMAC			x	x			x						
FCS_RND.1			x	x	x		x						
FIA_AFL.1/eID-PIN_Suspending		x	x	x	x								
FIA_AFL.1/eID-PIN_Blocking		x	x	x	x	x							
FIA_AFL.1/PACE						x							
FIA_API.1/CA			x	x	x		x						
FIA_UID.1/PACE			x	x	x								
FIA_UID.1/Rightful_Terminal		x	x	x	x								
FIA_UAU.1/PACE			x	x	x								
FIA_UAU.1/Rightful_Terminal		x	x	x	x								
FIA_UAU.1/SSCD[200]												x	x
FIA_UAU.4			x	x	x								
FIA_UAU.5			x	x	x								
FIA_UAU.6			x	x	x								
FDP_ACC.1/TRM		x	x		x								
FDP_ACF.1/TRM		x	x		x								
FDP_RIP.1		x	x	x	x		x						
FTP_ITC.1/PACE						x							
FTP_ITC.1/CA			x	x	x	x							

[200] this item is applicable, if the *eSign* application is operational.

	OT.Identification	OT.Personalisation	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.ID_Card_Tracing	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.SCD/SVD_Gen [7][200]	OT.Sigy_SigF [7][200]
FAU_SAS.1	x	x											
FMT_SMF.1	x	x	x	x	x								
FMT_SMR.1	x	x	x	x	x								
FMT_LIM.1								x					
FMT_LIM.2								x					
FMT_MTD.1/INI_ENA	x	x											
FMT_MTD.1/INI_DIS	x	x											
FMT_MTD.1/CVCA_INI			x	x	x								
FMT_MTD.1/CVCA_UPD			x	x	x								
FMT_MTD.1/DATE			x	x	x								
FMT_MTD.1/PA_UPD		x	x	x	x		x						
FMT_MTD.1/SK_PICC			x	x	x		x						
FMT_MTD.1/KEY_READ			x	x	x		x						
FMT_MTD.1/eID-PIN_Resume		x	x	x	x								
FMT_MTD.1/eID-PIN_Unblock		x	x	x	x								
FMT_MTD.1/eID-PIN_Activate		x	x	x	x								
FMT_MTD.3			x	x	x								
FPT_EMSEC.1									x				
FPT_FLS.1									x		x		
FPT_TST.1									x		x		
FPT_PHP.3			x						x	x			

Table 14: Coverage of Security Objectives for the TOE by SFR

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

242 The security objective **OT.Identification** addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip.
This will be ensured by TSF according to SFR FAU_SAS.1.
The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life phase 'operational use'.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

243 The security objective **OT.Personalisation** aims that only Personalisation Agent can write the User- and the TSF-data into the TOE (it also includes installing/activating of the *eSign* application).
This property is covered by FDP_ACC.1/TRM and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorisation level of a rightful terminal. This authorisation level can be achieved by the terminal identification/authentication as required by the SFR FIA_UID.1/Rightful_Terminal, FIA_UAU.1/Rightful_Terminal[201]. Since only an ATT can reach the necessary authorisation level, using and management of eID-PIN (FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking, FMT_MTD.1/eID-PIN_Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data.
FMT_MTD.1/PA_UPD covers the related property of OT.Personalisation (updating SO_C).
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

244 The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the Terminal- and the Chip Authentication, of these data exchanged (physical manipulation and unathorised modifying).
Physical manipulation is addressed by FPT_PHP.3.
Unathorised modifying of the stored data is addressed, in the first line, by FDP_ACC.1/TRM and FDP_ACF.1/TRM. A concrete authorisation level is achieved by the terminal identification/authentication as required by the SFRs FIA_UID.1/Rightful_Terminal, FIA_UAU.1/Rightful_Terminal (is supported by FCS_COP.1/SIG_VER). The TA protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use eID-PIN as the shared secret, using and management of eID-PIN (FIA_AFL.1/eID-PIN_Suspending, FIA_AFL.1/eID-PIN_Blocking, FMT_MTD.1/eID-PIN_Resume, FMT_MTD.1/eID-PIN_Unblock, FMT_MTD.1/eID-PIN_Activate) also support achievement of this objective. FDP_RIP.1 requires erasing the temporal values of eID-PIN, eID-PUK.
FIA_UAU.4, FIA_UAU.5 and FCS_CKM.4 represent some required specific properties of the protocols used.
To allow a verification of the certificate chain as required in FMT_MTD.3, the CVCA's public key and certificate as well as the current date are written or update by authorised identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.
Unathorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/CA using FCS_COP.1/CMAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication FIA_API.1/CA using FCS_CKM.1/DH_CA and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for K_{MAC}).
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalisation Agent only and, hence, is to consider as trustworthily.

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

The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

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

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

This objective for the data exchanged is mainly achieved by FTP_ITC.1/CA using FCS_COP.1/AES. A prerequisite for establishing this trusted channel is a successful Chip Authentication FIA_API.1/CA using FCS_CKM.1/DH_CA and FCS_CKM.2/DH and possessing the special properties FIA_UAU.5, FIA_UAU.6. The CA provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires to make this key unreadable for a user, so that its value remains confidential. FDP_RIP.1 requires erasing the values of SK_{PICC} and session keys (here: for K_{Enc}).
FMT_MTD.1/PA_UPD requires that SO_C containing, amongst other, signature over the PK_{PICC} and used for the Passive Authentication is allowed to be modified by the Personalisation Agent only and, hence, is to consider as trustworthily.
The SFRs FCS_COP.1/SHA and FCS_COP.1/RND represent the general support for cryptographic operations needed.
The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related.

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

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

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

250 The security objective **OT.Prot_Inf_Leak** aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE.
This objective is achieved
- by FPT_EMSEC.1 for measurement and analysis of the shape and amplitude of signals or the

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

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

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

253 The rationale related to the security functional requirements taken over from [7] (incl. OT.SCD/SVD_Gen, OT.Sigy_SigF and FIA_UAU.1/SSCD) are exactly the same as given for the respective items of the security policy definitions in sec. 11.1 of [7].

6.3.2 Rationale for SFR's Dependencies

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

255 The dependency analysis has directly been made within the description of each SFR in sec. 6.1 above. All dependencies being expected by CC part 2 and by extended components definition in chap. 5 are either fulfilled or their non-fulfilment is justified.

256 The rationale for SFR's dependencies related to the security functional requirements taken over from [7] are exactly the same as given for the respective items of the security policy definitions in sec. 11.2 of [7].

6.3.3 Security Assurance Requirements Rationale

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

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

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

260 The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 4, entry 'Attacker'). This decision represents a part of the conscious security policy for the ID_Card required by the ID_Card Issuer and reflected by the current PP.

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

262 The augmentation of EAL4 chosen comprises the following assurance components:

– ALC_DVS.2,

– ATE_DPT.2 and

– AVA_VAN.5.

263 For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package:

Component	**Dependencies required by CC Part 3 or ASE_ECD**	**Dependency fulfilled by**
TOE security assurance requirements (only additional to EAL4)		
ALC_DVS.2	no dependencies	-
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 15: SAR Dependencies

6.3.4 Security Requirements – Internal Consistency

264 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

265 The analysis of the TOE´s security requirements with regard to their mutual supportiveness and internal consistency demonstrates:

The dependency analysis in section 6.3.2 ‘Rationale for SFR’s Dependencies’ for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items.

The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 ‘Security Assurance Requirements Rationale’ shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

266 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.2 ‘Rationale for SFR’s Dependencies’ and 6.3.3 ‘Security Assurance Requirements Rationale’. Furthermore, as also discussed in section 6.3.3 ‘Security Assurance Requirements Rationale’, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 Glossary and Acronyms

Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the ID_Card's chip to produce Terminal Certificates with the correct certificate effective date, see [11], sec. 2.2.5.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the ID_Card's chip to store the Initialisation Data and Pre-personalisation Data.
Authentication terminal (ATT)	A technical system being operated and used either by a governmental organisation (Official Domestic Document Verifier) or by any other, also commercial organisation and (i) verifying the ID_Card presenter as the ID_Card holder (using the secret eID-PIN[202]), (ii) updating a subset of data of the eID application and (iii) activating the eSign application. See also par. 23 above and [11], chap. 3.2 and C.4. For the *eSign* application, it is equivalent to CGA as defined in [7].
Authenticity	Ability to confirm that the ID_Card itself and the data elements stored in were issued by the ID_Card Issuer
Basic Access Control	Security mechanism defined in [8] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
Basic Inspection System (BIS)	A technical system being used by an authority[203] and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying correspondence between the stored and printed MRZ. BIS implements the terminal's part of the Basic Access Control protocol and authenticates itself to the ID_Card using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (ID_Card document details data and biographical data) stored on the ID_Card (ePassport application only). See also *Application note 4*, [11], chap. G.1 and H; also [8].
Biographical data (biodata)	The personalised details of the ID_Card holder appearing as text in the visual and machine readable zones of and electronically stored in the ID_Card. The biographical data are less-sensitive data.
Biometric reference	Data stored for biometric authentication of the ID_Card holder in the ID_Card as (i) digital portrait and (ii) optional biometric reference data.

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

[203] concretely, by a control officer

Term	Definition
data	
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Identification Card), semi-static (e.g. printed on a label on the Identification Card) or dynamic (randomly chosen by the electronic ID_Card and displayed by it using e.g. ePaper, OLED or similar technologies), see [11], sec. 3.3
Card Security Object (SO_C)	An RFC3369 CMS Signed Data Structure signed by the Document Signer (DS). It is stored in the ID_Card (EF.CardSecurity, see [11], table A.1 and sec. A.1.2) and carries the hash values of different Data Groups as defined in [11], Appendix A. It shall also carry the Document Signer Certificate (C_{DS}), [11], A.1.2.
Certificate chain	Hierarchical sequence of Terminal Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Certification Service Provider (CSP)	An organisation issuing certificates or providing other services related to electronic signatures. There can be 'common' CSP, who cannot issue qualified certificates and 'qualified' CSP, who can also issue qualified certificates. A CSP is the Certification Service Provider in the sense of [7].
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means. [8]
Country Signing CertA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ID_Card Issuer with respect to confirming correctness of user and TSF data stored in the ID_Card. The CSCA represents the country specific root of the PKI for the ID_Cards and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [8], 5.1.1. The CSCA issuing certificates for Document Signers (cf. [8]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [11], sec. 2.2.1
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the ID_Card Issuer with respect to protection of user data stored in the ID_Card (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the rightful terminals (EIS, ATT, SGT) and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [11], chap. 2.2.1.

Term	Definition
	The CSCA issuing certificates for Document Signers (cf. [8]) and the domestic CVCA may be integrated into a single entity, e.g. a Country CertA. However, even in this case, separate key pairs must be used for different roles, see [11], sec. 2.2.1
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 [11], sec. 2.2.5.
CV Certificate	Card Verifiable Certificate according to [11], appendix C.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Digital Signature	according to the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on "*a Community framework for electronic signatures*" a digital signature qualifies as an electronic signature, if it is: - uniquely linked to the signatory; - capable of identifying the signatory; - created using means that the signatory can maintain under his sole control, and - linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Document Details Data	Data printed on and electronically stored in the ID_Card representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the ePassport application of the ID_Card. It may carry the Document Signer Certificate (C_{DS}); see [8].
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the ID_Card Security Object stored on the ID_Card for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [11], chap. 1.1 and [8]. This role is usually delegated to the Personalisation Agent.
Document Verifier (DV)	An organisation (certification authority) enforcing the policies of the CVCA and of a service provider (governmental or commercial organisation) and managing the terminals belonging together (e.g. terminals operated by a State's border police) by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a CertA, authorised by at least the national CVCA to issue certificates for national terminals, see [11], chap. 2.2.2. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the ID_Card Issuer; a foreign

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

Term	Definition
	DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the ID_Card Issuer und a foreign CVCA ensuring enforcing the ID_Card Issuer's privacy policy[204]).
Eavesdropper	A threat agent reading the communication between the ID_Card and the Service Provider to gain the data on the ID_Card.
eID application	A part of the TOE containing the non-executable, related user data and the data needed for authentication; this application is intended to be used for accessing official and commercial services, which require access to the user data stored in the context of this application. See [11], sec. 3.1.2.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity; see [8].
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [11], sec. 3.1.1.
eSign application	A part of the TOE containing the non-executable data needed for generating advanced or qualified electronic (concretely: digital) signatures on behalf of the ID_Card holder as well as for authentication; this application is intended to be used in the context of official and commercial services, where an advanced or qualified digital signature of the ID_Card holder is required. The eSign application is optional: it means that it can optionally be activated[205] on the ID_Card by a Certification Service Provider (or on his behalf) using the ATT with an appropriate effective authorisation level. See [11], sec. 3.1.3.
Extended Access Control	Security mechanism identified in [8] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorised to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System (EIS)	See *Inspection system*
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [8].
General Authentication Procedure	A specific order of authentication steps between an ID_Card and a terminal as required by [11], sec. 3.4, namely (i) PACE, (ii) Terminal Authentication (version 2), (iii) Passive Authentication and (iv) Chip Authentication (version 2).
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all MRTDs; see [8].

[205] ‚activated' means (i) generate and store in the *eSign* application one or more signature key pairs and (ii) optionally store there the related certificates

Term	Definition
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
ID_Card (electronic)	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally)
ID_Card holder	The rightful/legitimated holder of the electronic ID Card for whom the issuing authority personalised the ID Card.
ID_Card Issuer (issuing authority)	Organisation authorised to issue an electronic Identity Card to the ID_Card holder
ID_Card presenter	A person presenting the ID_Card to a terminal and claiming the identity of the ID_Card holder.
Identity Card (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Identity Card is used in order to verify that identity claimed by the Identity Card presenter is commensurate with the identity of the Identity Card holder stored on/in the card.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document; see [8].
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [8].
Initialisation Data	Any data defined by the ID_Card manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as IC_Card material (IC identification data).
Inspection	The act of an authority examining an ID_Card presented to it by an ID_Card presenter and verifying its authenticity as the ID_Card holder. See also [8].
Inspection system (EIS)	A technical system being used by an authority[206] and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the ID_Card presenter as the ID_Card holder (for *ePassport*: by comparing the real biometrical data of the ID_Card presenter with the stored biometrical data of the ID_Card holder). The specification [11], sec. 3.2 (and C.4) knows only one type of the inspection system, namely according to the result of the terminal authentication in the context of the General Authentication Procedure. It

[206] concretely, by a control officer

Term	Definition
	means that the Inspection System in the context of [11] (and of the current PP) is commensurate with the Extended Inspection System (EIS) as defined in [6][207]. See also par. 23 above.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The ID_Card's chip is an integrated circuit.
Integrity	Ability to confirm the ID_Card and its data elements stored upon have not been altered from that created by the ID_Card Issuer.
Issuing Organisation	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [8].
Issuing State	The country issuing the MRTD; see [8].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [8]. The capacity expansion technology used is the MRTD's chip.
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [8].
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods; see [8]. The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for both PACE and BAC.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine; see [8].
Malicious equipment	A technical device not possessing a valid, certified key pair for its authentication; validity of its certificate is not verifiable up to the respective root CertA (CVCA for a terminal and CSCA for an ID_Card).
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the ID_Card Manufacturer completing the IC to the ID_Card. The Manufacturer is the default user of the TOE during the manufacturing life phase[208]. The TOE itself does not distinguish between the IC Manufacturer and ID_Card Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [11], sec. C.1.3. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template,

[207] please note that an Extended Inspection System also covers the General Inspection Systems (GIS) in the sense of [6]

[208] cf. also par. 14 in sec. 1.2.3 above

Term	Definition
	- Certificate Effective Date, - Certificate Expiration Date, - Certificate Extensions (optional).
PACE Terminal (PCT)	A technical system verifying correspondence between the stored password and the related value presented to the terminal. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ID_Card using a shared password (CAN, MRZ, eID-PIN, eID-PUK). The PCT is not allowed reading User Data (see sec. 4.2.2 in [11]). See [11], chap. 3.3, 4.2, table 1.2 and G.2.
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card (Document) Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card (Document) Security Object. See [11], sec. 1.1.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [11], sec. 4.2. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personal Identification Number (PIN)	A short secret password being only known to the ID_Card holder. PIN is a blocking password, see [11], sec. 3.3.
Personalisation	The process by which the individual-related data (biographic and biometric data, signature key pair(s) for the eSign application) of the ID_Card holder are stored in and unambiguously, inseparably associated with the ID_Card.
Personalisation Agent	An organisation acting on behalf of the ID_Card Issuer to personalise the ID_Card for the ID_Card holder by some or all of the following activities: (i) establishing the identity of the ID_Card holder for the biographic data in the ID_Card[209], (ii) enrolling the biometric reference data of the ID_Card holder[210], (iii) writing a subset of these data on the physical Identification Card (optical personalisation) and storing them in the ID_Card (electronic personalisation) for the ID_Card holder as defined in [11], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Card Security Object defined in [8] (in the role of DS). A Personalisation Agent acts, amongst other, as the Document Signer (item (vi) of his tasks). Generating signature key pair(s) is not in the scope of the tasks of this role.
PIN Unblock Key (PUK)	A long secret password being only known to the ID_Card holder. The PUK is a non-blocking password, see [11], sec. 3.3.
Pre-personalisation	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised ID_Card and/or to

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

210 relevant for the ePassport application

Term	Definition
Data	secure shipment within or between the life cycle phases *manufacturing* and *card issuing*.
Pre-personalised ID_Card's chip	ID_Card's chip equipped with a unique identifier and a unique asymmetric Authentication Key Pair of the chip.
Receiving State	The Country to which the ID_Card holder is applying for entry; see [8].
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Remote terminal	A remote device directly communicating with the TOE and using the technical infrastructure between them (Internet, a local RF-terminal) merely as a message carrier. Only after Chip Authentication when a secure end-to-end connection between the TOE and remote terminal is established, the TOE grants access to the data of the eID application, see [11], sec. 3.4.1.
Restricted Identification	Restricted Identification aims providing a temporary ID_Card identifier being specific for a terminal sector (pseudo-anonymisation) and supporting revocation features (sec. 2.3, 4.1.2, 4.5 of [11]). The security status of ID_Card is not affected by Restricted Identification.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443
Rightful equipment (rightful terminal or rightful ID_Card)	A technical device possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either EIS or ATT or SGT. A terminal as well as an ID_Card can represent the rightful equipment, whereby the root CertA for a terminal is CVCA and for an ID_Card – CSCA.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [8].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service Provider	An official or commercial organisation providing services which can be used by the ID_Card holder. Service Provider uses the rightful terminals managed by a DV.
Signature terminal (SGT)	A technical system used for generation of digital signatures. See also par. 23 above and [11], chap. 3.2 and C.4. It is equivalent – as a general term – to SCA and HID as defined in [7].
Skimming	Imitation of a rightful terminal to read the ID_Card or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ, CAN, eID-PIN or eID-PUK data.
Terminal	A technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as neither PCT nor EIS nor ATT nor SGT ('Terminal' is used by the ID_Card presenter).
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country

Term	Definition
	Verifying Certification Authority which shall be all valid for the Current Date. It can additionally be restricted at terminal by ID_Card holder using CHAT.
TOE tracing data	Technical information about the current and previous locations of the ID_Card gathered by inconspicuous (for the ID_Card holder) recognising the ID_Card
Travel document	A passport or other official document of identity issued by a State or Organisation which may be used by the rightful holder for international travel; see [8].
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised ID_Card	ID_Card material prepared to produce a personalised ID_Card containing an initialised and pre-personalised ID_Card's chip.
User Data	All data (being not authentication data) stored in the context of the applications of the ID_Card as defined in [11] and (i) being allowed to be *read out* or *written* solely by an authenticated terminal (in the sense of [11], sec. 3.2) respectively (ii) being allowed to be *used* solely by an authenticated terminal (in the sense of [11], sec. 3.2) (the private Restricted Identification key; since the Restricted Identification according to [11], sec. 4.5 represents just a functionality of the ID_Card, the key material needed for this functionality and stored in the TOE is considered here as 'user data') respectively (iii) being allowed to be *used* solely by the authenticated ID_Card holder (the private signature key within the eSign application; from this point of view, the private signature key of the ID_Card holder is also considered as 'user data'). CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
ATT	Authentication Terminal as defined in [11], sec. 3.2
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority (the author dispensed with the usual abbreviation 'CA' in order to avoid a collision with 'Chip Authentication')
CGA	Certificate generation application, please refer to [7]. In the current context, it is represented by ATT for the eSign application.
CHAT	Certificate Holder Authorization Template
DTBS	Data to be signed, please refer to [7]
DTBS/R	Data to be signed or its unique representation, please refer to [7]
EAC	Extended Access Control
EIS	Extended Inspection System (equivalent to the Inspection Systems as defined in [11], sec. 3.2)
GAP	General Authentication Procedure (see [11], sec. 3.4)
HID	Human Interface Device, please refer to [7]. It is equivalent to SGT in the current context.
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PCT	PACE-authenticated terminal
PICC	Proximity Integrated Circuit Chip
PIN	Personal Identification Number
PP	Protection Profile
PUK	PIN Unblock Key
RAD	Reference Authentication Data, please refer to [7]
RF	Radio Frequency
SAR	Security assurance requirements
SCA	Signature creation application, please refer to [7]. It is equivalent to SGT in the current context.
SCD	Signature Creation Data, please refer to [7]; the term 'private signature key within the eSign application' is synonym within the current PP.
SFR	Security functional requirement
SGT	Signature Terminal as defined in [11], sec. 3.2
SVD	Signature Verification Data, please refer to [7]

Acronym	Term
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)
VAD	Verification Authentication Data, please refer to [7]

8 Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

Protection Profiles

[5] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, version 1.10, 25th March 2009

[6] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009

[7] Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-1:2009, ver. 1.03, 2009-12, BSI-CC-PP-0059-2009

ICAO

[8] ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In *Machine Readable Travel Documents – Part 1: Machine Readable Passport*, volume 2, ICAO, 6th edition, 2006

[9] ICAO Doc 9303-3, Specifications for electronically enabled official travel documents with biometric identification capabilities. In *Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents*, volume 2, ICAO, 3rd edition, 2008.

Technical Guidelines and Directives

[10] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[11] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), TR-03110, version 2.02, 09.11.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, version 1.00, 2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[14] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

Cryptography

[15] Übersicht über geeignete Algorithmen: Bekanntmachung zur Elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, 17.11.2008, Veröffentlicht am 27.01.2009 im Bundesanzeiger Nr. 13, S. 346

[16] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[17] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

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

[19] Secure hash standard (and Change Notice to include SHA-224), FIPS PUB 180-2, National Institute of Standards and Technology, 2002

Other Sources

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