Security Target - ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration

Document Information

Author:	Thomas Aichinger Austria Card Ges.m.b.H.
Title:	Security Target
Version:	1.02 public
Date:	2021-11-29
Company:	AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Vienna, Austria
Classification:	**Public**

Document History

Version	Date	Author	Changes
v1.02	2021-11-29	AC	Public version

1 Contents

2 Security Target Introduction (ASE_INT)

2.1 ST Reference

Title	Security Target - ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration
Version	1.02 public
Author	Austria Card Ges.m.b.H.
Compliant to	Common Criteria Protection Profiles: • "Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE" (EAC PP) [1] and • "Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) [2]
CC Version	3.1 Revision 5
Certification ID ANSSI	ACOS-ID
Assurance Level	EAL4+
Keywords	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)

2.2 TOE Reference

TOE Name	ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration
TOE Developer	Austria Card Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Wien, Austria
IC Developer	Infineon Technologies AG
TOE Hardware	Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13, BSI-DSZ-CC-1110-V4-2021
TOE Version	v2.0 eMRTD (B)

2.3 TOE Overview

This ST defines the security objectives and requirements for the contact based / contactless chip of electronic documents (i.a., machine readable travel documents – MRTD, driving license) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO), EU requirements for biometric European passport [3] and Biometric European Resident Permit [4]. It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication and optionally Active Authentication according to "ICAO Doc 9303" [5].

ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration is a chip operating system compliant to ISO 7816-3 [6], ISO 7816-4 [7], ISO 7816-8 [8], ISO 7816-9 [9], ISO 14443 [10] [11] [12] , BSI TR03110 [13] and EN 419212 [14] for secure chips used in electronic documents (MRTD). It provides multi-application support (e.g. Signature-, Access Control-, Health-Applications). The operating system runs on Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13 including software packages [15].

The secure chip and software packages (e.g. libraries) are certified according to CC EAL 6+ according to the Protection Profile BSI-CC-PP-0084-2014 [16] (see [17]).

The TOE is a composition of ACOS-IDv2.0 operating system and applications (software) and a secure chip (hardware) including its associated software packages (software).

2.4 TOE Description

2.4.1 TOE Definition

The Target of Evaluation (TOE) is a secure chip including software for an electronic document to be included in e.g. a machine readable travel document representing a contactless / contact passport or smart card programmed according to ICAO Technical Report "Supplemental Access Control" / "PACE" [18] / [5] (which means amongst others according to the Logical Data Structure (LDS) and additionally providing the Extended Access Control according to the "ICAO Doc 9303" [5] and [13], respectively. The communication between terminal and secure chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), [2]. For PACE the "generic mapping" and the "integrated mapping" are supported. Additionally, Active Authentication according to "ICAO Doc 9303" [5] is provided.

The TOE provides multi-application support, i.e., installation of additional multi-purpose applications (MPA) is possible.

The TOE supports contact based T=1 (according ISO/IEC7816-3) and contactless T=CL Type A (according to ISO/IEC14443) communication protocols.

The following "Figure 1: TOE Block Diagram" gives an overview of the TOE and its borders and the scope of the evaluation.

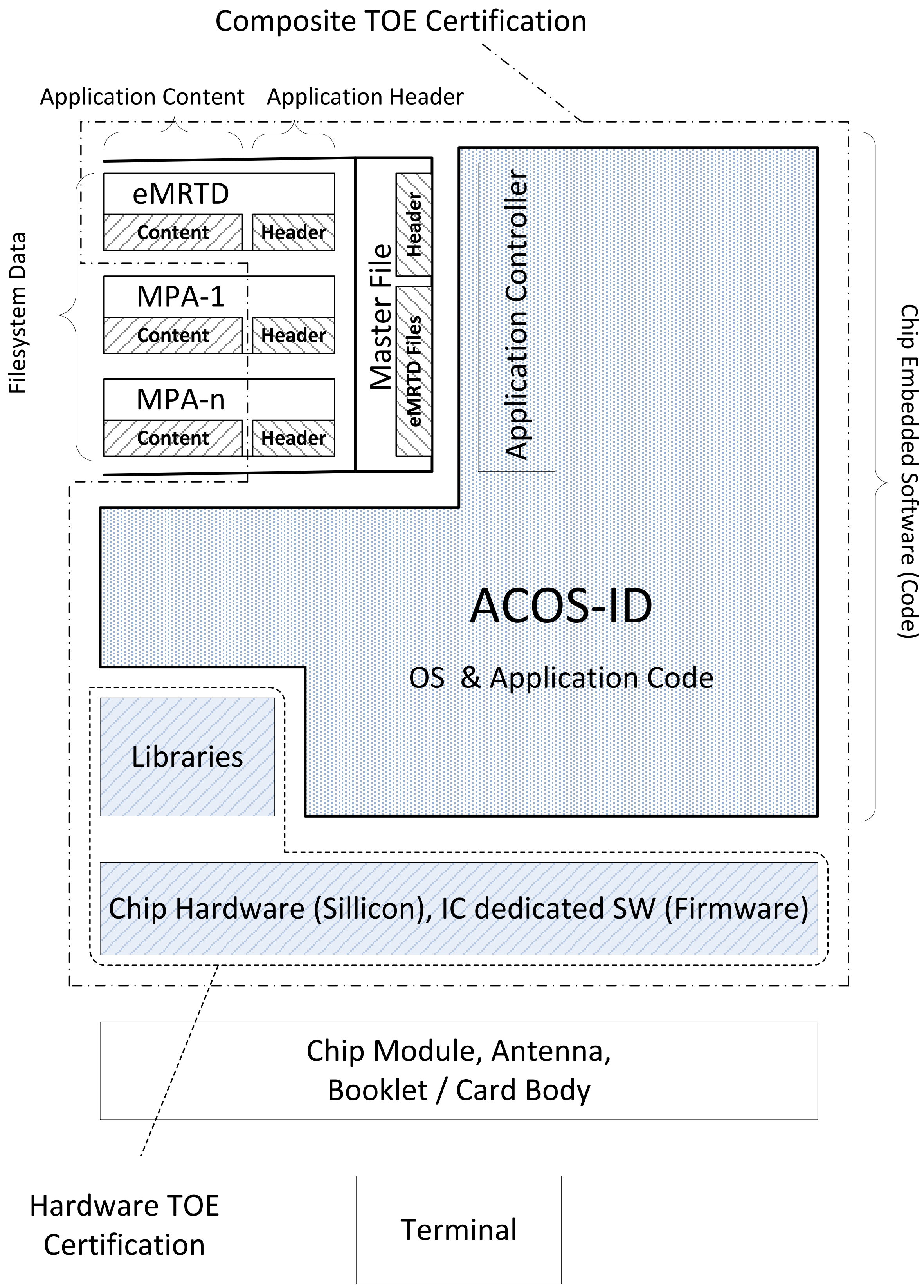


Figure 1: TOE Block Diagram

2.4.2 Scope

"Figure *1: TOE Block Diagram*" together with "*Table 1:* Components and Scope" define the scope of the TOE. The latter gives more details and also divided the physical versus the logical scope.

Component	**In Scope of TOE (physical / logical)**	**Covered by**
Chip Hardware (Silicon) and IC dedicated Software (Firmware)	Yes (physical)	Chip hardware certification
Libraries (from secure chip hardware vendor)	Yes (logical)	Chip hardware certification
ACOS-ID Operation System and Application Code (IC Embedded Software) including Application Controller	Yes (logical)	Composite certification
Master File, application header and eMRTD related files / keys	Yes (logical)	Composite certification
eMRTD, MPA-1 … MPA-n Application Header	Yes (logical)	Composite certification
eMRTD Application Content, including file/key headers	Yes (logical)	Composite certification
Guidance Documentation	Yes (physical)	Composite certification
MPA-1 … MPA-n Application Content	No	n/a
Chip Module, Bonding Wires, Antenna, Booklet / Card Body (all optional)	No	n/a
Terminal	No	n/a

Table 1: Components and Scope

From the communication (Operating System to Terminal) perspective the logical scope ends at the input / output interface of the Operating System, which is the APDU-Interface (Application Protocol Data Unit) consisting of all commands supported by the operating system. Any APDU command is received by the input interface and any response APDU is sent via the output interface.

All commands and responses are physically transmitted over either the contact-based or the contactless hardware interface, represented by connections on the Chip Hardware (pads on silicon).

2.4.3 TOE Usage and Security Features for Operational Use

A State or Organisation issues electronic documents incorporated into machine readable travel documents to be used by the holder for international travel, as well as similar electronic documents incorporated in documents such as driving license, electronic health card or other proprietary applications. This Security Target covers the application where the traveller presents a machine readable travel document or a driving license to the inspection system to prove his or her identity. The machine readable travel document contains

(i) visual (eye readable) biographical data and portrait of the holder,
(ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
(iii) data elements on the travel document's chip (electronic document) according to LDS in case of contactless machine reading.

The authentication of the traveller is based on

(i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and
(ii) biometrics using the reference data stored in the travel document.

The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

The travel document is viewed as unit of

(i) the **physical part of the travel document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
    a. the biographical data on the biographical data page of the travel document surface,
    b. the printed data in the Machine Readable Zone (MRZ) and
    c. the printed portrait.
(ii) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [5] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder
    a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
    b. the digitized portraits (EF.DG2),
    c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
    d. the other data according to LDS (EF.DG5 to EF.DG16) and
    e. the Document Security Object (SOD).

The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [5]. These security measures can include the binding of the travel document's chip to the travel document.

The logical travel document is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organisation and the security features of the travel document's chip

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [5], and Password Authenticated Connection Establishment [5]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This ST addresses the protection of the logical travel document

(i) in integrity by write-only-once access control and by physical means, and
(ii) in confidentiality by the Extended Access Control Mechanism.

This ST addresses the Chip Authentication Version 1 described in [13] **and** the Active Authentication stated in [5].

BAC is additionally supported by the composite product, but it is not in the scope of this ST due to the fact that [19] only considers extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3). Therefore a separate evaluation and certification process using an ST [20] conformant to [19] is carried out contemporaneous to the current process.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document strictly conforms to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [2]. Note that [2] considers high attack potential.

For the PACE protocol according to [5], the following steps shall be performed:

- (i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
- (ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
- (iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.
- (iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [13], [5].

The TOE implements the Extended Access Control as defined in [13]. The Extended Access Control consists of two parts

- (i) the Chip Authentication Protocol Version 1 and
- (ii) the Terminal Authentication Protocol Version 1 (v.1).

The Chip Authentication Protocol v.1

- (i) authenticates the travel document's chip to the inspection system and
- (ii) establishes secure messaging

which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed.

The Terminal Authentication Protocol v.1 consists of

- (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and
- (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

The TOE supports both PACE mapping methods "generic mapping" and "integrated mapping" as defined in [13] (but no "chip authentication mapping").

The secure messaging established by the PACE protocol is preserved to protect the data transmission from the TOE to the inspection system.

The TOE implements as an option Active Authentication (AA) according to [5] part 1 vol. 2 NORMATIVE APPENDIX 4 using ECDSA. AA may be used in addition to Chip Authentication followed by Terminal Authentication. It can also be used instead of Chip Authentication to ensure the authenticity of the Chip – but in this case Terminal Authentication cannot be performed. (see also notes (1), (2), (3) and (4) below).

Notes:

1. PP56 [1] addresses the Chip Authentication Version 1 described in [13] as an alternative to the Active Authentication stated in [5].
2. This ST refines PP56 [1] and addresses the Chip Authentication Version 1 described in [13] and optionally the Active Authentication stated in [5].
3. Active Authentication is optional because the Active Authentication Public Key data can be stored in DG15 (EF.DG15) as well as the private key can be installed or not. If the Active Authentication Public Key data and the private key is not stored, Active Authentication is not available and vice versa.
4. Chip Authentication Version 1 protocol and Active Authentication protocol both authenticate the Travel document's Chip to the terminal.

The TOE can also be used as a driving license (IDL or eDL) compliant to ISO/IEC 18013 [21] or ISO/IEC TR 19446 [22] (according Commission Regulation (EU) No 383/2012 [23]) supporting PACE, AA and CA, as both applications (MRTD and IDL/eDL) share the same protocols and data structure organization. Therefore, in the rest of the document, the word “MRTD” may be understood either as a MRTD in the sense of ICAO, or a driving license compliant to ISO/IEC 18013 or ISO/IEC TR 19446 depending on the targeted usage envisioned by the issuer.

When an Issuer is using the product as a driving licence, the following name mapping of roles, definitions, data groups and protocol is applicable within the scope of this security target:

MRTD	Driving License or eDL or IDL
ICAO	ISO/IEC
ICAO 9303	ISO/IEC 18013 or ISO/IEC TR 19446
BAC	BAP-1
DG3	DG7*
DG4	DG8*
DG15	DG13
MRZ	MRZ or SAI (Scanning area identifier)
Traveller	Holder

*Access rights of DG3 and DG4 (containing the biometric data) are also mapped to DG7 and DG8, respectively.

Multi-Application support

Beside the travel document application the additional multi-purpose applications (MPA) may be optionally installed. To ensure that the security objectives of the MRTD still hold, restrictions and minimum requirements for the MPA applications (e.g. necessary access conditions for contained files, keys) are defined and evaluated to prove their correctness as a part of the evaluation. The main restriction for MPAs is that only a BIS-Authenticated Terminal (after successful performing the PACE protocol) is able to select any MPA application. The application separation (access control / access conditions) provided by the OS ensures that no inference with the ePassport application is possible.

2.4.4 TOE Life-Cycle

The description of the TOE life-cycle includes the four life-cycle phases and 7 steps exactly as given in the PP [1] and extends it by addition of a fifth life-cycle phase. Additional Notes are inserted into the original text taken from the PP where necessary, e.g. to explain the two delivery options which are introduced below.

The mapping of the roles is defined as follows:

- IC developer: Infineon Technology AG (as defined by the IC Certificate)
- IC Manufacturer: Production Sites in charge of Infineon (as defined by the IC Certificate)
- IC Embedded Software Developer: Austria Card Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Wien, Austria (Development Site as covered by Site Certificate BSI-DSZ-CC-S-0153)
- Travel Document Manufacturer: any entity authorized by Austria Card

The TOE makes use of a Flash-Technology IC product in combination with “Loader functionality” (provided by the “secure flash loader package” of the IC / IC dedicated software), which is a dedicated secure method, covered by the IC certification , see also “Package Loader, Package 1” and “Package Loader, Package 2” acc. [24]) to load the IC Embedded Software. The IC Security Target [24] addresses this topic in “P.Lim_Block_Loader” and “P.Ctrl_Loader”. See also [24] Annex 7, especially Table 17 and Application Note 32.

Delivery Options:

IC Embedded Software (ACOS-ID Operation System and Application Code, Libraries) will only reside in non-volatile programmable memory (Flash). Therefore the IC Embedded Software may either be written by

- Option a) the IC Manufacturer or by
- Option b) the Travel Document Manufacturer making use of the “Loader functionality”

In both cases Austria Card delivers the Guidance Documentation of the TOE (including ePassport application TSF data), initialization data as well as necessary keys to the Travel Document Manufacturer. Additionally

in case of Option a)

- the IC including the IC embedded software is delivered to the Document Manufacturer

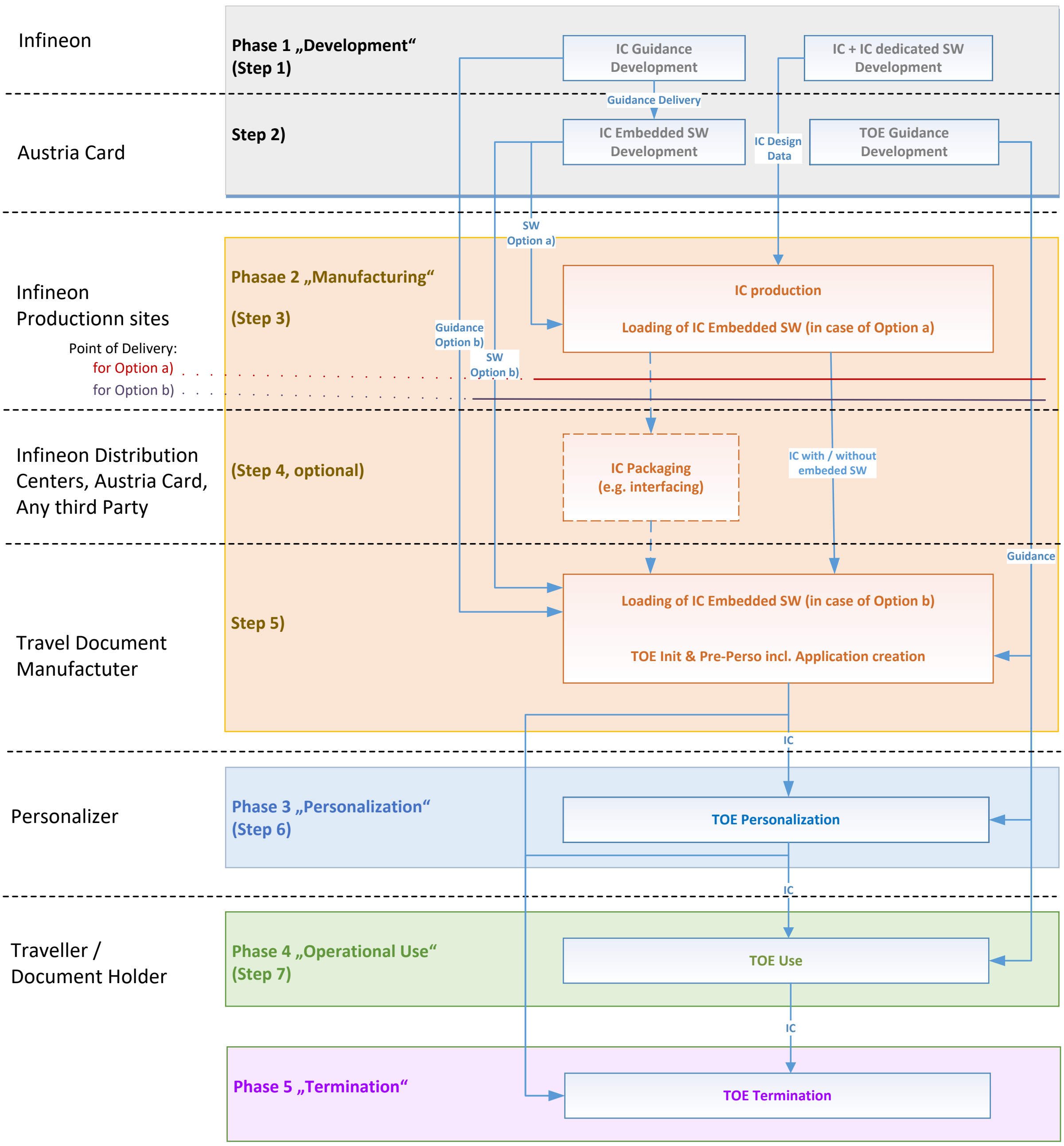
in Case of Option b)

- the IC Embedded Software is delivered from Austria Card to the Document Manufacturer.
- the IC without the IC embedded software is delivered to the Document Manufacturer
- For acceptance, processing of the IC and loading the Travel Document Manufacturer follows the Guidance Documentation of the IC
- Directly after successfully loading the IC Embedded Software the TOE exists for the first time and the Travel Document Manufacturer follows the guidance documentation of the TOE.

For both Options the IC is delivered from Production Sites via “Distribution Centers” – both in charge of Infineon (as defined in the IC certification) - to the Document Manufacturer or from Production Sites via “Distribution Centers” – both in charge of Infineon (as defined in the IC certification) - to Austria Card and from Austria Card to the Document Manufacturer.

The life-cycle description is taken from the underlying PP [1] (four life-cycle phases and 7 steps) and complemented by a fifth life-cycle phase and additional notes explaining the delivery options.

The following picture gives an overview of the life-cycle of the TOE. Details are given below.



<u>Phase 1 “Development”</u>

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC

Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer.

Note: The term ”non-volatile non-programmable memories” typically refers to ROM, where the non-programmable (ROM) part can only be “written” by the IC Manufacturer during Mask-processing. The TOE does uses Flash technology instead, so the “Embedded Software in the non-volatile non-programmable memories“ part does not exists. In case of

- Option a) the IC Embedded Software is securely delivered to the IC Manufacturer (via IC Developer Infineon) or
- Option b) the IC Embedded Software is securely delivered to the travel document manufacturer.

The ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

Note: the term “ePassport application” above refers mainly to application data (TSF data, part of the guidance documentation) but not to executable code. Whole executable code is part of the Operating System and Application code or libraries.

Phase 2 “Manufacturing”

(Step3) In a first step the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software and the parts[1] of the travel document’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.

If necessary (Note: which means in case of Option a)), the IC manufacturer adds the parts of the IC Embedded Software in the non- volatile programmable memories (Flash). Note: in Case of Option a) the TOE exists after this action.

The IC is securely delivered from the IC manufacturer to the travel document manufacturer. Note: The delivery can optionally be done via the IC Developer Infineon and Austria Card. In Case of

- Option a) this step is the TOE delivery, while in case of
- Option b) the IC is delivered without the IC Embedded Software and therefore the delivered ICs does not represent the TOE (the IC Embedded Software is delivered to the Document Manufacturer separately)

(Step 4 optional) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the card only.

Note: Step 4 may be performed by any entity action on behalf of the travel document manufacturer.

(Step5) The travel document manufacturer

(i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (FLASH) if necessary (Note: this is necessary only in case of Option b) when this was not done before by the IC manufacturer),

[1] Note: for this TOE such parts don’t exist; no part of the IC Embedded Software is contained in ROM.

(ii) creates the ePassport application (create the MF and ICAO.DF[2]), and
(iii) equips travel document's chips with pre- personalization Data.
(iv) Note: optionally the travel document manufacturer equips travel document's chip with personalization data such as
  a. Initial CVCA Public Key
  b. Initial CVCA Certificate
  c. Initial Current Date

  But this can instead also be done in phase 3 by the Personalization Agent.

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

Phase 3 "Personalisation of the travel document"

(Step6) The personalisation of the travel document includes

(i) the survey of the travel document holder's biographical data,
(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
(iii) the personalization of the visual readable data onto the physical part of the travel document,
(iv) the writing of the TOE User Data and TSF Data into the logical travel document and
(v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of

(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2),
(iii) the Document security object, and
(iv) personalization data such as
  a. Initial CVCA Public Key
  b. Initial CVCA Certificate
  c. Initial Current Date

  Note: the personalization with the initial CVCA Public Key, Certificate and Current Date can instead also be done in phase 2 by the manufacturer.

The signing of the Document security object by the Document signer [13] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

The TSF data[3] (data created by and for the TOE, that might affect the operation of the TOE) comprise (but are not limited to) the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

This ST distinguishes[4] between the Personalisation Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [5]. This approach allows but does not enforce the separation of these roles.

---

[2] See Application Note 1 of [1]
[3] See also Application Note 2 from PP56v2

Phase 4 “Operational Use”

(Step7) The TOE is used as a travel document's chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified.

Phase 5 “Terminated”

If the TOE’s security mechanisms observe an attack, critical operating environment conditions or a malfunction it shuts itself down permanently. This state can be reached any time after the IC Embedded Software (operating system) has been installed and started (from phase 2, 3 or phase 4 on) and is final. Encrypted log data can be read that allow tracing back to cause of the shut-down.

This ST considers the phases 1 and parts of phase 2 (Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after Step 3[5].

The production, generation and installation procedures (step 4, 5, 6 as applicable) after TOE delivery up to the “Operational Use” (Phase 4) and “Terminated” (Phase 5) have been considered in the product evaluation process under AGD assurance class.

2.4.5 Non-TOE Hardware/Software/Firmware Required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip (sillicon) and the complete operating system and application code and ePassport application data. Note, the module (including bonding wires) holding the chip as well as the antenna and the booklet (holding the printed MRZ) or card body are needed to represent a complete travel document, nevertheless these parts are irrelevant for the secure operation of the TOE.

[4] See also Application Note 3 from PP56v2

[5] See also Application Note 4 from [1]

2.4.6 TOE Components

The TOE consists of the following components:

Category	Definition
Secure Chip Hardware	Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13
Secure Chip Firmware	80.100.17.3, 80.100.17.2
Secure Chip Vendor Software Libraries	Crypto Library (ACL): v2.08.007 Hardware Support Layer (HSL): 03.12.8812
Operating System	ACOS-IDv2.0 Builds: 0x8C1D, 0x62D7 and 0x9486 Those builds differ in their support of different configurations of the same TOE Hardware (RAM Size, User NVM Size, availability of the Very High Bit Rate (VHBR) feature). The builds and the underlying code are represented by the label “REL_ACOS-IDv2.0_01” in the repository. This chip embedded software version corresponds to the Version Identifier “v2.0” of the TOE (part of the TOE name).
Guidance Documentation	The Guidance consists of the following documents: • “Preparation and Operational Manual - ACOS-IDv2.0 eMRTDv2.0, BAC and EAC/PACE Configuration”, Version 1.04, Date 2021-11-29, [25] • “ACOS-ID User Manual”, Version 2.12, Date 19.05.2021 [26] • “Internal Operation Manual - ACOS-IDv2.0”, Version 1.2, 2021-07-19, [27] (only used Austria Card internal) Those documents are represented by the label “REL_ACOS-IDv2.0_eMRTD_CC-DOC_02” in the repository. This documentation version is reflected by the text “eMRTD (B)” part of the TOE name, where “eMRTD” refers to documentation for a specific type of certification and “(B)” to the specific version of the documentation.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Revision 5, [28] [29] [30] as follows:

Part 2 extended due to the use of

- FAU_SAS.1
- FCS_RND.1
- FMT_LIM.1
- FMT_LIM.2
- FPT_EMS.1

from [2] and

- FIA_API.1. from [1],

Part 3 conformant.

For the evaluation the following methodology is used: [31]

3.2 PP Claim

This Security Target claims strict conformance to the Protection Profiles

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP) [1]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) [2]

3.3 Package claim

This Security Target is conforming to assurance package EAL4 augmented with:

- ALC_DVS.2
- ATE_DPT.2
- AVA_VAN.5

due to PP68 [2].

And additionally:

- ALC_FLR.1
- ALC_CMS.5
- ALC_TAT.2

as defined in CC part 3 [30].

3.4 Conformance Claim Rationale

This Security Target claims strict conformance to the following protection profiles as required:

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP) [1]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) [2]

The chapter Security Problem Definition (ASE_SPD) is taken over from the claimed PPs without changes.

The chapter Security Objectives (ASE_OBJ) is taken over from the claimed PPs completely and extended by

- Proof of the travel document's chip authenticity

With Proof of the travel document's chip authenticity the Active Authentication functionality is introduced.

Active Authentication is a challenge-response protocol defined in [5]:

- the terminal sends a challenge (nonce) to the chip
- the chips sends a signature of this nonce to the terminal

- and the terminal verifies this signature.

Active Authentication allows cryptographic verification of the authenticity of the chip and is an alternative to Chip Authentication which performs a public key exchange for the same purpose. The keys used for Active Authentication are different from the keys used by Chip Authentication.

OE.AA_Key_Travel_Document Travel document Authentication Key

With OE.AA_Key_Travel_Document Travel document Authentication Key the issuing State or Organization has to establish the necessary public key infrastructure to make the Active Authentication functionality possible.

Conclusion:

1. The OT added to content of the PPs in the ST do not change the statement of Security Objectives of the PPs
2. The statement of Security Objectives in this ST remains consistent with the statement of Security Objectives in the PPs.

The chapter Extended Component Definition (ASE_ECD) is taken over from the claimed PPs without changes.

The chapter Security Requirements (ASE_REQ) is taken over from the claimed PPs completely without changes but the following security requirements are added:

- **FCS_CKM.1/AA_EC_KeyPair**

The SFR introduces functionality to this ST which

- adds the key generation functionality for Active Authentication to this TOE, which
  - is an alternative mechanism to Chip Authentication
  - works with its own key pair which is different from the CA key pair

Conclusion:

- The SFR added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

- **FCS_CKM.1/CA_EC_KeyPair**

The SFR introduces functionality to this ST (according to [1] Application Note 44) which

- adds the key generation functionality for Chip Authentication to this TOE, which
  - is an alternative mechanism to generating the key externally and loading it onto the TOE
  - works with its own key pair which is different from the AA key pair

Conclusion:

- The SFR added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
- The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

- **FCS_COP.1/AA_SGEN_EC**
  The SFR introduces functionality to this ST which
    - adds the signature generation functionality for Active Authentication to this TOE which needs a private key which might either be created by FCS_CKM.1/AA_EC_KeyPair (see above) or loaded.
    - is an alternative mechanism to Chip Authentication

  Conclusion:
    - The SFR added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
    - The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

- **FIA_API.1/AA**
  The SFR introduces functionality to this ST which
    - adds the Active Authentication functionality to this TOE
    - works with its own key pair which is different from the CA key pair

  Conclusion:
    - The SFR added to content of the PPs in the ST do not change the statement of SFRs in the PPs.
    - The statement of SFRs in this ST remains consistent with the statement of SFRs in the PPs.

4 Security Problem Definition (ASE_SPD)

4.1 Introduction

This ST introduces optional functionality (Active Authentication) as an alternative to Chip Authentication.

For the purpose of authentication of the chip to the terminal the Chip Authentication and Active Authentication are equivalent mechanisms. Therefore and since those parts taken from [1] already consider Chip Authentication there is no modification of the SPD needed.

4.2 Assets

The assets to be protected by the TOE include the User Data on the travel document's chip, user data transferred between the TOE and the terminal, and travel document tracing data from the claimed PACE PP [7], chap 3.1.:

Primary Assets (User Data)

Asset	Definition
User data stored on the TOE	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [5] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [5]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [19].
User data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [5] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [5]). User data can be received and sent (exchange ⇔ {receive, send}).
Travel document tracing data	Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.
Logical travel document sensitive User Data	Sensitive biometric reference data (EF.DG3, EF.DG4).
Authenticity of the travel document's chip	The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.

Table 2: Primary Assets

Secondary Assets (TSF Data)

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.
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

	[19].
TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.
Travel document communication establishment authorisation data	Restricted-revealable authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.

4.3 Subjects

This ST includes all subjects from [1] (which itself includes all these subjects from [2]).

Travel document holder	A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [19]. Please note that a travel document holder can also be an attacker (s. below).
Travel document presenter (traveller)	A person presenting the travel document to a terminal 22 and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [19]. Please note that a travel document presenter can also be an attacker (s. below).
Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [19].
Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [5]. This role is usually delegated to a Personalisation Agent.

Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document 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. [5], 5.5.1.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [5], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [5] (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 travel document Issuer. This entity is commensurate with 'Personalisation agent' in [19].
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [19].
Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the ST, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [19]. A threat agent trying

	(i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document.
Country Verifying Certification Authority (CVCA)	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link- Certificates.
Document Verifier (DV)	The Document Verifier enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the travel document in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates.
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining a travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Extended Inspection System	The Extended Inspection System performs the Advanced Inspection Procedure (see [1], figure 1) and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [5] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

	Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

4.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. This ST includes all assumptions from [1] and [2].

A.Insp_Sys	**Inspection Systems for global interoperability**
The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [4] and/or BAC [8]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. **Justification:** The assumption A.Insp_Sys does not confine the security objectives of the [7] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.	

A.Auth_PKI	**PKI for Inspection Systems**
The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip. **Justification:** This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [7] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.	

A.Passive_Auth	**PKI for Passive Authentication**
The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores	

and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [6].

4.5 Threats

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

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Read_Sensitive_Data	**Read the sensitive biometric reference data**
Adverse action:	An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [19]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.
Threat agent:	having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document.
Asset:	confidentiality of logical travel document sensitive user data (i.e. biometric reference).

T.Counterfeit	**Counterfeit of travel document chip data**
Adverse action:	An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents.
Asset:	authenticity of user data stored on the TOE.

T.Skimming	**Skimming travel document / Capturing Card-Terminal**
Adverse action:	An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance
Asset:	confidentiality of logical travel document data
Application Note	This TOE does not support BAC.
Application Note	A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 10 of [2]).
Application Note	MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder. (cf. application note 11 of [2]).

T.Eavesdropping	**Eavesdropping on the communication between the TOE and the PACE terminal**
Adverse action:	An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
Asset:	confidentiality of logical travel document data
Application Note	This TOE does not support BAC.
Application Note	A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST (cf. application note 12 of [2]).

T.Tracing	**Tracing travel document**
Adverse action:	An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.
Threat agent:	having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
Asset:	privacy of the travel document holder
Application Note	This threat completely covers and extends "T.Chip-ID" from BAC PP [BSI-CC-PP-0055-110]. (cf. application note 13 of [2]).
Application Note	A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST. (cf. application note 14 of [2])
Application Note	Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document’s chip (no Chip Authentication or Active Authentication), a threat like

	T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE. (cf. application note 15 of of [2])

T.Forgery	**Forgery of Data**
Adverse action:	An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart (i) the PACE authenticated BIS-PACE or (ii) the authenticated Extended Inspection System[6] by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.
Threat agent:	having high attack potential.
Asset:	integrity of the travel document.

T.Abuse-Func	**Abuse of Functionality2**
Adverse action:	An attacker may use functions of the TOE which shall not be used in TOE operational phase in order 1. to manipulate or to disclose the User Data stored in the TOE, 2. to manipulate or to disclose the TSF-data stored in the TOE or 3. to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the travel document holder.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents.
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document.
Application Note	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 (cf. application note 16 of [2]).

T.Information_Leakage	**Information Leakage from travel document**
Adverse action:	An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.
Threat agent:	having high attack potential.
Asset:	confidentiality of User Data and TSF-data of the travel document
Application Note	Leakage may occur through emanations, variations in power

[6] T.Forgery is extended by (ii) due to PP [1] Application note 8.

	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). (cf. application note 17 of [2]).

T.Phys-Tamper	**Physical Tampering**
Adverse action:	An attacker may perform physical probing of the travel document in order 1. to disclose the TSF-data, or 2. to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter 1. its security functionality (hardware and software part, as well), 2. the User Data or the TSF-data stored on the travel document.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents.
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.
Application Note	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 travel document) 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 travel document'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. (cf. application note 18 of [2]).

T.Malfunction	**Malfunction due to Environmental Stress**
Adverse action:	An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to

	1. deactivate or modify security features or functionality of the TOE's hardware or to 2. circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation. attacker needs information about the functional operation.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation.
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.
Application Note	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. (cf. application note 19 of [2]).

4.6 Organizational Security Policies

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.

The following OSP are taken directly from [1] which itself includes P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal taken from [8].

P.Sensitive_Data	**Privacy of sensitive biometric reference data**
The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.	

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

P.Manufact	**Manufacturing of the travel document's chip**
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.	
Note	OSP P.Manufact covers OSP "P.Process-TOE" of [32] which inherits OSP "P.Process-TOE" from PP [24]

P.Pre-Operational	**Pre-operational handling of the travel document**
1. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations. 2. The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE, see Primary assets and Secondary assets. 3. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, see TOE Life-Cycle above. 4. If the travel document Issuer authorizes a Personalization Agent to personalize the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the travel document Issuer's policy.	

P.Card_PKI	**PKI for Passive Authentication (issuing branch)**
Note	The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services. (cf. application note 20 of [2]).
1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}) . 2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [5], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [5], 5.5.1. 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 and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.	

<table>
<tr><td>P.Trustworthy_PKI</td><td>Trustworthiness of PKI</td></tr>
<tr><td colspan="2">The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.</td></tr>
</table>

<table>
<tr><td>P.Terminal</td><td>Abilities and trustworthiness of terminals</td></tr>
<tr><td colspan="2">The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:
1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [5].
2. They shall implement the terminal parts of the PACE protocol [5], of the Passive Authentication [5] and use them in this order[7]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [5]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.</td></tr>
<tr><td>REFINEMENT</td><td>P.Terminal holds also for Extended Inspection System with PACE.</td></tr>
</table>

[7] This order is commensurate with [5].

5 Security Objectives (ASE_OBJ)

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

5.1 Security Objectives for the TOE

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

The following Objectives are taken directly from [1] which itself includes OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.Prot_Abuse-Func, OT.Prof_Inf_Leak, OT.Prot_Phys-Tamper, OT.Identification, OT.AC_Pers and OT.Prot_Malfunction taken from [8].

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

OT.Chip_Auth_Proof	**Proof of the travel document's chip authenticity**
The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [13]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.	
Note	The OT.Chip_Auth_Proof implies the travel document's chip to have I. a unique identity as given by the travel document's Document Number, II. a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by I. the Chip Authentication Public Key (EF.DG14) in the LDS defined in [5] and II. the hash value of DG14 in the Document Security Object signed by the Document Signer. (cf. Application Note 9 from [1])

OT.Data_Integrity	**Integrity of Data**
The TOE must ensure integrity of the User Data and the TSF-data[8] 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 during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.	
Refinement	**OT.Data_Integrity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.**

OT.Data_Authenticity	**Authenticity of Data**
The TOE must ensure authenticity of the User Data and the TSF-data[9] stored on it by enabling verification of their authenticity at the terminal-side[10]. The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[11].	
Refinement	**OT.Data_Authenticity holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.**

OT.Data_Confidentiality	**Confidentiality of Data**
The TOE must ensure confidentiality of the User Data and the TSF-data[12] by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.	
Refinement	**OT.Data_Confidentiality holds also for Extended Inspection System which has used an authenticated BIS-PACE for authentication.**

OT.Tracing	**Tracing travel document**
The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.	
Note **(REFINED)**	**Since this TOE supports Chip Authentication**, a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)

[8] See Secondary Assets
[9] See Secondary Assets
[10] Verification of SO_D
[11] secure messaging after the PACE authentication, see also [5]
[12] See Secondary Assets

	can be achieved by the current TOE. (cf. application note 21 of [2]).

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 1. to manipulate or to disclose the User Data stored in the TOE, 2. to manipulate or to disclose the TSF-data stored in the TOE, 3. to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.	

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 travel document • by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, • by forcing a malfunction of the TOE and/or • by a physical manipulation of the TOE.	
Note	This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker (cf. application note 2 of [2]).

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 travel document's Embedded Software by means of • measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or • measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis), • manipulation of the hardware and its security functionality, as well as • controlled manipulation of memory contents (User Data, TSF-data) with a prior • reverse-engineering to understand the design and its properties and functionality.	

OT.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.

OT.Identification	**Identification of the TOE**
The TOE must provide means to store Initialization[13] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).	

OT.AC_Pers	**Access Control for Personalization of logical MRTD**
The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [5] and the TSF data can be written by authorized Personalization Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.	
Note	The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization. (cf. application note 23 of [2]).

The following threat has been included in addition to the threats in the protection profiles:

OT.Active_Auth_Proof	**Proof of travel document's chip authenticity**
The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [5]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.[14]	

5.2 Security Objectives for the Operational Environment

Travel document Issuer as the general responsible

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

OE.Legislative_Compliance	**Issuing of the travel document**
The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.	

[13] amongst other, IC Identification data
[14] REFINEMENT

OE.Auth_Key_Travel_Document	**Travel document Authentication Key**
The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.	
Justification	This security objective for the operational environment is needed additionally to those from [2] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE.

OE.AA_Key_Travel_Document	**Travel document Authentication Key**
The issuing State or Organisation has to establish the necessary public key infrastructure in order to (iv) generate the travel document's **Active Authentication Key Pair**, (v) sign and store the **Active Authentication Public Key** data in **EF.DG15** and (vi) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the **Active Authentication Public** Key by means of the Document Security Object.	

OE.Authoriz_Sens_Data	**Authorization for Use of Sensitive Biometric Reference Data**
The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.	
Justification	This security objective for the operational environment is needed additionally to those from [2] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre- requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in [1] and not in [2].

Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Passive_Auth_Sign	**Authentication of travel document by Signature**
The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). 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 Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [5]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [5]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.	

OE.Personalisation	**Personalisation of travel document**
The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [5] (see also , [5], sec. 10) (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [6] (in the role of a DS).	

Terminal operator: Terminal's receiving branch

OE.Terminal	**Terminal operating**
The terminal operators must operate their terminals as follows: 1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [5]. 2.) The related terminals implement the terminal parts of the PACE protocol [5], of the Passive Authentication [5] (by verification of the signature of the Document Security Object) and use them in this order[15] . The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).	

[15] This order is commensurate with [5].

3.) The related terminals need not to use any own credentials. 4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [5]). 5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.	
Note	OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [19]. See note 24 from [2].

Travel document holder Obligations

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

Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives of the TOE environment.

OE.Exam_Travel_Document	**Examination of the physical part of the travel document**
The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [5] and/or the Basic Access Control [5]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.	
Justification	This security objective for the operational environment is needed additionally to those from [2] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [2] and therefore also counters T.Forgery and A.Passive_Auth from [2]. This is done because a new type of Inspection System is introduced in [1] as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.
Refinement	Inspection Systems not able to perform EAC perform additionally to these points Active Authentication (if optionally available and the terminal's ability allows to perform AA) to verify the Authenticity of the presented travel document's chip.

OE.Prot_Logical_Travel_Document	**Protection of data from the logical travel document**
The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.	
Justification	This security objective for the operational environment is needed additionally to those from [2] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Ext_Insp_Systems	**Authorization of Extended Inspection Systems**
The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.	
Justification	This security objective for the operational environment is needed additionally to those from [2] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre- requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

5.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	*OT.Active_Auth_Proof*	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Identification*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*	OE.Auth_Key_Travel_Document	OE.AA_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	*OE.Personalisation*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*
T.Read_Sensitive_Data	x															x			x					
T.Counterfeit		x	x											x	x		x							

T.Skimming					x	x	x																x	
T.Eavesdropping							x																	
T.Tracing								x															x	
T.Abuse-Func									x															
T.Information_Leakage										x														
T.Phys-Tamper												x												
T.Malfunction													x											
T.Forgery				x	x	x			x			x					x			x	x	x		
P.Sensitive_Data	x															x			x					
P.Personalisation				x							x									x				
P.Manufact											x													
P.Pre-Operational				x							x									x				x
P.Terminal																	x					x		
P.Card_PKI																					x			
P.Trustworthy_PKI																					x			
A.Insp_Sys																	x	x						
A.Auth_PKI																x			x					
A.Passive_Auth																	x				x			

The Objectives, threats and assumptions marked in italic letters are included from PACE-PP [2].

The OSP **P.Personalisation** “Personalisation of the travel document by issuing State or Organisation only” addresses the

(i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** “Personalisation of logical travel document”, and

(ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document”.

Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation Agent.

The OSP **P.Sensitive_Data** “Privacy of sensitive biometric reference data” is fulfilled and the threat **T.Read_Sensitive_Data** “Read the sensitive biometric reference data” is countered by the TOE-objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data” requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

The OSP **P.Terminal** “Abilities and trustworthiness of terminals” is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [2].

OE.Exam_Travel_Document enforces the terminals to perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** “Counterfeit of travel document chip data” addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip identification and authenticity proof required by **OT.Chip_Auth_Proof** or OT.Active_Auth_Proof “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organisation. The Active Authentication Public Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.AA_Key_Travel_Document** “Travel document Authentication Key”. The Chip Authentication Public Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** “Travel document Authentication Key”. According to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” the General Inspection system has to perform the **Active Authentication Protocol or** the Chip Authentication Protocol [16] to verify the authenticity of the travel document’s chip.

The threat **T.Forgery** “Forgery of data” 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 terminal. Additionally to the security objectives from PACE PP [2] which counter this threat, the examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

The examination of the travel document addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document’s chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** “Protection of data from the logical travel document” require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

The assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** “Authentication of travel document by Signature” from PACE PP [2] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_Travel_Document** “Examination of the physical part of the travel document”.

The assumption **A.Auth_PKI** “PKI for Inspection Systems” is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data” requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems” to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

[16] REFINEMENT Active Authentication Protocol

6 Extended Component Definition (ASE_ECD)

6.1 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the 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.

Note: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API	**Authentication Proof of Identity**
Family behaviour	
This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.	
Component levelling:	
FIA_API Authentication Proof of Identity	1
FIA_API.1	Authentication Proof of Identity
Management:	FIA_API.1
The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.	
Audit:	There are no actions defined to be auditable.

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

6.2 Definition of the Family FAU_SAS

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.

FIA_SAS	**Audit Storage**
Family behaviour	
This family defines functional requirements for the storage of audit data.	
Component levelling:	
FAU_SAS Audit data storage	1
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 dependencie
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

6.3 Definition of the Family FCS_RND

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. 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 Generation of random numbers	1
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].

6.4 Definition of the Family FMT_LIM

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.

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 Limited capabilities and availability	1 and 2
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	**FMT_LIM.1**
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].
Application Note 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 1. 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 2. 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.	

6.5 Definition of the Family FPT_EMS

The family FPT_EMS (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 [29].

FPT_EMS	TOE emanation
Family behaviour	
This family defines requirements to mitigate intelligible emanations.	
Component levelling:	
FPT_EMS TOE emanation	1
FPT_EMS.1	TOE emanation has two constituents:
FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMS.1
There are no management activities foreseen	
Audit:	FPT_EMS.1
There are no actions defined to be auditable.	

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of*

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

7 Security Requirements (ASE_REQ)

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [28] of the CC.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “refinement” in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the ST authors are denoted as underlined text and the original text of the component is given by a footnote.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the ST authors are denoted by showing as underlined text and the original text of the component is given by a footnote.

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.

7.1.1 Subjects

The definition of the subjects

- Manufacturer,
- Personalisation Agent,
- Extended Inspection System,
- Country Verifying Certification Authority,
- Document Verifier
- Terminal

used in the following chapters is given in section Subjects.

7.1.2 Objects

All used objects are defined in section Glossary.

7.1.3 Security Attributes

Security Attribute	Values	Meaning
Terminal Authentication Status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [13]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [13]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [13]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [13]); Terminal is

		authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [5])
	DG3 (Fingerprint)	Read access to DG3: (cf. [5])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [5])

Notes:

1. Security attribute Terminal Authentication Status is spelled differently in PP [1], e.g. FDP_ACF.1/TRM spells it Terminal Authentication v.1.
2. Security attribute Terminal Authorization is spelled differently in PP [1], e.g. FDP_ACF.1/TRM spells it Authorization of the Terminal.
3. These different spellings are corrected by refinements to read always Terminal Authentication Status or Terminal Authorization.

7.1.4 Keys and Certificates

The following table provides an overview of the keys and certificates used. Where PP [2] is more specific than PP [1] name and data are taken from PP [2].

Keys and certificates taken from PP56 [1]

Key/Certificate Name	Meaning
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material by the TOE in order to enforce its security functionality.
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. The PK.CVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C.CVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [13] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK.CVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes
Document Verifier Certificate (C.DV)	The Document Verifier Certificate C.DV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK.DV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, (iii) the Certificate Effective Date and the Certificate

	Expiration Date as security attributes.
Inspection System Certificate (C.IS)	The Inspection System Certificate (C.IS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK.IS), (ii) the coded access control rights of the Extended Inspection System, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK.ICC, PK.ICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [33].
Chip Authentication Public Key (PK.ICC)	The Chip Authentication Public Key (PK.ICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK.ICC)	The Chip Authentication Private Key (SK.ICC) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Chip Authentication Session Keys (CA-K.MAC, CA-K.Enc)	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System as result of the Chip Authentication Protocol Version 1.

Keys and certificates taken from PP68 [2]

Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the travel document Issuer signs the Document Signer Public Key Certificate (C.DS) with the Country Signing Certification Authority Private Key (SK.CSCA) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK.CSCA). The CSCA also issues the self-signed CSCA Certificate (CCSCA) to be distributed by strictly secure diplomatic means, see [5], 5.5.1
Document Signer Key Pairs and Certificates	The Document Signer Certificate C.DS is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK.DS) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO.D) of the travel document 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).
PACE Session Keys (PACE-K.MAC, PACE-K.Enc)	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [5].
PACE authentication ephemeral key pair (ephem-SK.PICC.PACE, ephem-	The ephemeral PACE Authentication Key Pair {ephem-SK.PICC.PACE, ephem- PK.PICC-PACE } is used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman (ECDH; ECKA key

PK.PICC.PACE)	agreement algorithm) according to TR-03111 [34], cf. [5].
Active Authentication Key Pair	The Active Authentication Key Pair (KPr.AA, KPu.AA) are used for Active Authentication Protocol according to [5] part 1 vol. 2 chapter "7.2.2 Inspection process flow" section "Active Authentication (Optional)" using EC.
Active Authentication Public Key (KPu.AA)	The Active Authentication Public Key (KPu.AA) is stored in the EF.DG15 of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key (KPr.AA)	The Active Authentication Private Key (KPr.AA) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Notes:

1. The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organization.
2. With the optional Active Authentication a key pair is stored in the chip.
3. According to OE.AA_Key_Travel_Document the hash value of ACTIVE AUTHENTICATION PUBLIC KEY INFO (cf. [5] part 1 vol.2 chapter NORMATIVE APPENDIX 4) is stored in the Document Security Object (SO.D) for verifying the key using Passive Authentication.

7.2 SFR Class FAU

7.2.1 SFRs from PP BSI-CC-PP-0068-V2-2011

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records.
Application Note The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase ‘manufacturing’. The IC manufacturer and the travel document 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 travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.	

7.3 SFR Class FCS

7.3.1 SFRs from PP BSI-CC-PP-0068-V2-2011

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 fulfilled by FCS_CKM.2/DH. Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [35][17] and specified cryptographic key sizes 256, 384, 512, 521[18] that meet the following: [5][19].
Application Note The TOE generates a shared secret value K with the terminal during the PACE protocol, see [5] This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [36]) or on the ECDH compliant to TR- 03111 [35] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [5] and [35] for details). The shared secret value K is used	

[17] [selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [35]]
[18] [assignment: cryptographic key sizes]
[19] [assignment: cryptographic key sizes] that meet the following: [5]]

for deriving the AES or DES session keys for message encryption and message authentication (PACE-K MAC, PACE-K Enc) according to [5] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. Note: the PACE protocol defines three different "mapping" methods (see [5] chapt. 4.4: This SFR FCS_CKM.1/DH_PACE covers "generic mapping" (see [5] chapt. 4.4.3.3.1) and "integrated mapping" (see sect. 4.4.3.3.2) but not "chip authentication mapping" (see chapt. 4.4.3.3.3).

FCS_CKM.4	**Cryptographic key destruction – Session keys, PACE and CA 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 FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting with constant or random data[20] that meets the following: none[21]
Application Note The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.	

FCS_COP.1/PACE_ENC	**Cryptographic operation – Encryption / Decryption AES / TDES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/PACE_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm AES, TDES[22] in CBC mode and cryptographic key sizes

[20] [assignment: cryptographic key destruction method]
[21] [assignment: list of standards]
[22] [selection: AES, 3DES]

	112, 128, 192, 256 [23] bit that meet the following: compliant to [5].
Application Note This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc).	

FCS_COP.1/PACE_MAC	**Cryptographic operation – MAC**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE. FCS_CKM.4 Cryptographic key destruction: fulfilled byFCS_CKM.4.
FCS_COP.1.1/PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC (AES), Retail-MAC[24] (TDES) and cryptographic key sizes 112 (TDES), 128 (AES), 192 (AES), 256 (AES)[25] bit that meet the following: compliant to [5].
Application Note 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}). Note that in accordance with [5] the (two-key) Triple-DES could be used in Retail mode for secure messaging.	

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 PTG.3 according to AIS 31 [37][26].
Application Note This SFR requires the TOE to generate random numbers (random nonce) used for the	

[23] [selection: 112, 128, 192, 256]
[24] [selection: CMAC, Retail-MAC]
[25] [selection: 112, 128, 192, 256]
[26] [assignment: a defined quality metric]

authentication protocol (PACE) as required by FIA_UAU.4/PACE.

7.3.2 SFRs from PP BSI-PP-0056-V2-2012-132

FCS_CKM.1/CA	**Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH[27] and specified cryptographic key sizes 256, 320, 384, 512, 521[28] that meet the following: ECDH protocol compliant to [35][29].
Application Note FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [13]. *Application Note* The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [13]. This protocol may be based on the Diffie- Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [36]) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [35], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [13]). *Application Note* The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 (cf. [13]). The TOE may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [13] for details). *Application Note* The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [2] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) 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. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.	

[27] [assignment: cryptographic key generation algorithm]
[28] [assignment: cryptographic key sizes]
[29] [selection: based on the Diffie-Hellman key derivation protocol compliant to [36] and [13] , based on an ECDH protocol compliant to [35]]

FCS_COP.1/CA_ENC	**Cryptographic operation – Symmetric Encryption / Decryption**
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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm TDES in CBC mode, AES in CBC mode[30] and cryptographic key sizes 112 (TDES), 128 (AES), 192 (AES), 256 (AES)[31] that meet the following: 1. (CBC mode:) ISO/IEC 10116 [38]. 2. (TDES:) ISO/IEC 18033-3 [39]. 3. (AES:) FIPS PUB 197 [40][32].
Application Note This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.	

FCS_COP.1/SIG_VER	**Cryptographic operation – Signature verification by travel document**
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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA[33] and cryptographic key sizes 256, 384, 512,521[34] that meet the following: BSI TR-03111 [34][35].
Application Note 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 v.1 (cf. [5]). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge	

[30] [assignment: cryptographic algorithm]
[31] [assignment: cryptographic key sizes]
[32] [assignment: list of standards]
[33] [assignment: cryptographic algorithm]
[34] [assignment: cryptographic key sizes]
[35] [assignment: list of standards]

FCS_COP.1/AA_SGEN_EC	**Cryptographic operation – Signature generation for AA with EC**
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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AA_SGEN_EC	The TSF shall perform digital signature generation[36] in accordance with a specified cryptographic algorithm ECDSA[37] and cryptographic key sizes 256, 384, 512, 521[38] that meet the following: BSI TR-03111 [34][39].
Application Note 1. SFR FCS_COP.1/AA_SGEN_EC is added to contents of PPs [1] and [2]. 2. The signature generation is used to perform Active Authentication.	

FCS_COP.1/CA_MAC	**Cryptographic operation – MAC**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC for AES, RETAIL-MAC TDES[40] and cryptographic key sizes 112 (TDES), 128 (AES), 192 (AES), 256 (AES)[41] that meet the following: (AES): FIPS PUB 197 [40][42] (TDES): ISO/IEC 18033-3 [39]. (CMAC/RETAIL-MAC): ISO/IEC 9797-1 [41]
Application Note This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.	

---

[36] [assignment: list of standards]
[37] [assignment: cryptographic algorithm]
[38] [assignment: cryptographic key sizes]
[39] [assignment: list of standards]
[40] [assignment: cryptographic algorithm]
[41] [assignment: cryptographic key sizes]
[42] [assignment: list of standards]

Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

7.3.3 Additional SFRs (not from PPs)

FCS_CKM.1/AA_EC_KeyPair	**Cryptographic key generation – EC key pair for AA**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/AA_EC_KeyPair	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm EC key generation[43] and specified cryptographic key sizes 256, 320, 384, 512, 521[44] that meet the following: ANSI X9.62-2005 and ISO/IEC 15946-1:2002[45].
Application Note 1. FCS_CKM.1/AA_EC_KeyPair is added to contents of PPs [1] and [2]. 2. With FCS_CKM.1/AA_EC_KeyPair the TOE is able to create an EC key pair for Active Authentication.	

FCS_CKM.1/CA_EC_KeyPair	**Cryptographic key generation – EC key pair for CA**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA_EC_KeyPair	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm EC key generation[46] and specified cryptographic key sizes 256, 320, 384, 512, 521[47] that meet the following: ANSI X9.62-2005 and ISO/IEC 15946-1:2002[48].
Application Note 1. FCS_CKM.1/CA_EC_KeyPair is added to contents of PPs [1] and [2]. 2. With FCS_CKM.1/CA_EC_KeyPair the TOE is able to create an EC key pair for Chip Authentication.	

[43] [assignment: cryptographic key generation algorithm]
[44][assignment: cryptographic key sizes]
[45] [selection: based on the Diffie-Hellman key derivation protocol compliant to [36] and [13] , based on an ECDH protocol compliant to [35]]
[46] [assignment: cryptographic key generation algorithm]
[47][assignment: cryptographic key sizes]
[48] [selection: based on the Diffie-Hellman key derivation protocol compliant to [36] and [13] , based on an ECDH protocol compliant to [35]]

7.4 SFR Class FIA

7.4.1 SFRs from PP BSI-CC-PP-0068-V2-2011

FIA_AFL.1/PACE	**Authentication failure handling – PACE authentication using non-blocking authorisation data**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when 1-16[49] unsuccessful authentication attempts occur related to authentication attempts using the PACE password as shared password.
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall - activate authentication delay for following authentication attempts[50], starting with a delay of 1 second and exponentially growing.
Application Note The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [5]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[51] , 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[52] requiring an attack potential beyond high, so that the threat T.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 PACE passwords'.	

FIA_UAU.6/PACE	**Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions

[49] [assignment: positive integer number]
[50] [assignment: list of actions]
[51] ≥ 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.
[52] guessing CAN or MRZ, see T.Skimming above

	each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.
Application Note The PACE protocol specified in [4] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.	

7.4.2 SFRs from PP BSI-PP-0056-V2-2012-132

FIA_UID.1/PACE	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/PACE	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE Protocol according to [5], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to carry out the Chip Authentication Protocol v.1 according to [13] 5. to carry out the Terminal Authentication Protocol v.1 according to [13] 6. **to carry out the Active Authentication Protocol according to** [5] [53]. on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user
Application Note User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE). *Application Note PP56* In the life-cycle 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 travel document 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 proves the respective Terminal Authorisation Level as defined by the related policy (policies).	

[53] [assignment: list of TSF-mediated actions]

FIA_UAU.1/PACE	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE Protocol according to [5], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to identify themselves by selection of the authentication key 5. to carry out the Chip Authentication Protocol v.1 according to [13] 6. to carry out the Terminal Authentication Protocol v.1 according to [13] **7. to carry out the Active Authentication Protocol according to** [5][54]**.** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Application Note The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE). 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	

FIA_UAU.4/PACE	**Single-use authentication of the Terminals by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according to [5] 2. Authentication Mechanism based on **TDES and AES**[55]. 3. Terminal Authentication Protocol v.1 according to [13].

[54] [assignment: list of TSF-mediated actions]
[55] [selection: Triple-DES, AES or other approved algorithms]

Application Note
The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

FIA_UAU.5/PACE	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/PACE	The TSF shall provide 1. PACE Protocol according to [5], 2. Passive Authentication according to [5], 3. Secure messaging in MAC-ENC mode according to [5], 4. Symmetric Authentication Mechanism based on **AES** [56] 5. Terminal Authentication Protocol v.1 according to [13], **6. Active Authentication according to** [5] to support user authentication.
FIA_UAU.5.2/PACE	The TSF shall authenticate any user's claimed identity according to the following rules: 1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol. 2. The TOE accepts the authentication attempt as Personalisation Agent by **the Authentication Mechanism with Personalisation Agent Key(s)** [57] 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1. 4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 5. **none**[58]
Application Note The SFR FIA_UAU.5.1/PACE covers the definition in PACE PP [2] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in	

[56] [selection: Triple-DES, AES or other approved algorithms]
[57] [selection: the Authentication Mechanism with Personalisation Agent Key(s)]
[58] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

the current PP covers the definition in PACE PP [2] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

FIA_UAU.6/EAC	**Re-authenticating – Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/EAC	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.
Application Note The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [5] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user	

FIA_API.1/CA	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/CA	The TSF shall provide a Chip Authentication Protocol Version 1 according to [13] to prove the identity of the TOE.
Application Note: Due to the fact that there is a SFR added to this ST using AA for Authentication Proof of Identity the SFR "FIA_API.1" of [1] *is renamed to "FIA_API.1/CA".*	
Application Note This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [13]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [5]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).	

FIA_API.1/AA	**Authentication Proof of Identity**
Hierarchical to:	No other components.

Dependencies:	No dependencies.
FIA_API.1.1/AA	The TSF shall provide an Active Authentication Protocol according to [5] to prove the identity of the TOE.
Application Note: SFR FIA_API.1/AA is iterated from PP SFR FIA_API.1/CA ("FIA_API.1").	
Application Note This SFR requires the TOE to implement the Active Authentication Mechanism specified in [5]. The TOE computes a signature over a nonce received from the terminal, sends the signature to the terminal and the terminal verifies the signature.	

7.5 SFR Class FDP

7.5.1 SFRs from PP BSI-CC-PP-0068-V2-2011

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 deallocation of the resource from[59] the following objects: 1. Session Keys (immediately after closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K according to [5]), 3. **none**[60].
Application Note The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric (' any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.	

FDP_UCT.1/TRM	**Basic data exchange confidentiality – MRTD**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP to be able to

[59] [selection: allocation of the resource to, deallocation of the resource from]
[60] [assignment: list of objects]

	transmit and receive user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
FDP_UIT.1.1/TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

7.5.2 SFRs from PP BSI-PP-0056-V2-2012-132

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/TRM	The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document.
Application Note The SFR FIA_ACC.1.1 in this ST covers the definition in PACE PP [2] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.	

FDP_ACF.1/TRM	**Security attribute based access control**
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.
FDP_ACF.1.1/TRM	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE, c. Extended Inspection System; 2. Objects: a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document, b. data in EF.DG3 of the logical travel document, c. data in EF.DG4 of the logical travel document, d. all TOE intrinsic secret cryptographic keys stored in the travel document; 3. Security attributes: a. PACE Authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal;
FDP_ACF.1.2/TRM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [5] after a successful PACE authentication as required by FIA_UAU.1/PACE.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorise access of subjects to objects 1. based on the following additional rules: none.
FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document. 2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document. 3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM. 4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder

	authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM. 5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM. 6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application Note
The SFR FDP_ACF.1.1/TRM in this ST covers the definition in PACE PP [2] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [2]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in PACE PP [2] and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.
Application Note
The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [13]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.
Application Note
Please note that the Document Security Object (SO_D) stored in EF.SOD (see [6]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [5].
Application Note
FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

7.6 SFR Class FTP

7.6.1 SFRs from PP BSI-CC-PP-0068-V2-2011

FTP_ITC.1/PACE	**Inter-TSF trusted channel after PACE**
Hierarchical to:	No other components.
Dependencies:	Inter-TSF trusted channel after PACE
FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the

	Terminal.
Application Note The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel. *Application Note* 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 Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE. *Application Note* Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.	

7.7 SFR Class FMT

7.7.1 SFRs from PP BSI-CC-PP-0068-V2-2011

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalisation, 3. Personalisation 4. Configuration.

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/PACE
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.

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/PACE
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to read out the Initialisation Data and Pre-personalisation Data to the Personalisation Agent.
Application Note 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 cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.	

FMT_MTD.1/PA	**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/PACE
FMT_MTD.1.1/PA	The TSF shall restrict the ability to write the Document Security Object (SO_D) to the Personalisation Agent.
Application Note By writing SO_D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data	

7.7.2 SFRs from PP BSI-PP-0056-V2-2012-132

FMT_SMR.1/PACE	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1/PACE	The TSF shall maintain the roles 1. Manufacturer, 2. Personalisation Agent,

	3. Terminal, 4. PACE authenticated BIS-PACE. 5. Country Verifying Certification Authority, 6. Document Verifier, 7. Domestic Extended Inspection System, 8. Foreign Extended Inspection System
FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.
Application Note The SFR FMT_SMR.1.1/PACE in this ST covers the definition in PACE PP [2] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP. *Application Note* *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.*	

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks. and 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited availability (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery do not allow: 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed,

	3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.
Application Note The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy. *Application Note* The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.	

FMT_MTD.1/CVCA_INI	**Management of TSF data – Initialization of CVCA Certificate and Current Date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date, **4. none** to Manufacturer, **Personalization Agent**[61].
Application Note The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization	

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 FMT_SMR.1 Security roles
FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate

[61] [assignment: the authorised identified roles]

	to Country Verifying Certification Authority
Application Note The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [13]). The TOE updates its internal trust-point if a valid Country Verifying CA Link- Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [13]).	

FMT_MTD.1/DATE	**Management of TSF data – Current date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/DATE	The TSF shall restrict the ability to modify the Current date to 3. Country Verifying Certification Authority, 4. Document Verifier, 5. Domestic Extended Inspection System
Application Note The authorized roles are identified in their certificate (cf. [13]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [13]).	

FMT_MTD.1/CA_AA_PK	**Management of TSF data – CA and AA Private Key**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ CA_AA_PK	The TSF shall restrict the ability to create or load[62] the Chip Authentication Private Key **and the Active Authentication Private Key** to Personalization Agent[63].
Application Note Due to the fact that this SFR is refined with Active Authentication the SFR "FMT_MTD.1/CAPK" of [1] is renamed to "FMT_MTD.1/CA_AA_PK". The verb "load" means here that the Chip Authentication Private Key and the Active Authentication Private Key are generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Chip Authentication Private Key and Active Authentication	

[62] [selection: create, load]
[63] [assignment: the authorised identified roles]

Private Key is generated by the TOE itself. This TOE is able to generate the Chip Authentication Private Key, see FCS_CKM.1/CA_EC_KeyPair. This TOE is able to generate the Active Authentication Private Key, see FCS_CKM.1/AA_EC_KeyPair.

FMT_MTD.1/KEY_READ	**Management of TSF data – Key Read**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read the 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalisation Agent Keys **4. Active Authentication Private Key** to none

FMT_MTD.3	**Secure TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
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 v.1 and the Access Control.
Refinement: The certificate chain is valid if and only if **1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,** **2. the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE** **3. the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.** **The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended**	

Inspection System **The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.**
Application Note The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

7.8 SFR Class FPT

7.8.1 SFRs from PP BSI-CC-PP-0068-V2-2011

FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. **none.**[64].

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 at the conditions: • At reset / OS Startup: Integrity check of whole file system • On any use of TSF data and user data (e.g. use of a DG / EF or key): Integrity check of used TSF and user data • On any code execution: Integrity check of executed code [65] to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

[64] [assignment: list of types of failures in the TSF]
[65] [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]]

Application Note If the travel document'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 cycle 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.

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 to the TSF by responding automatically such that the SFRs are always enforced.
Application Note 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.	

7.8.2 SFRs from PP BSI-PP-0056-V2-2012-132

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit **variations in IC power consumption or electromagnetic emissions or variations in command execution time**[66] in excess of **non-useful information**[67] enabling access to 1. Chip Authentication Session Keys 2. PACE session keys (PACE-K_{MAC} , PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. **Manufacturer Keys, PACE Chip Authentication Private Keys and Modular Invert of Chip Authentication Key**, **Active Authentication Private Key**[68] 5. Personalisation Agent Key(s), 6. Chip Authentication Private Key and

[66] [assignment: types of emissions]
[67] [assignment: specified limits]
[68] [assignment: list of types of user data]

	7. EF.DG3 and EF.DG4
FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to 1. Chip Authentication Session Keys 2. PACE session keys (PACE-K_{MAC} , PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. **Manufacturer Keys, PACE Chip Authentication Private Keys and Modular Invert of Chip Authentication Key, Active Authentication Private Key**[69] 5. Personalisation Agent Key(s), 6. Chip Authentication Private Key and 7. **EF.DG3, EF.DG4**
Application Note 56 The SFR FPT_EMS.1.1 in the current PP covers the definition in PACE PP [2] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in the current PP covers the definition in PACE PP [2] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.	

7.9 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

augmented by taking the following components:

- ALC_DVS.2
- ATE_DPT.2
- AVA_VAN.5
- ALC_FLR.1
- ALC_CMS.5
- ALC_TAT.2

Application note: The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the PACE and / or Chip Authentication Protocol v.1 (see also OE.Prot_Logical_Travel_Document).

7.10 Security Requirements Rationale

7.10.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

[69] [assignment: list of types of TSF data]

	OT.Sens_Data_Conf.	OT. Chip_Auth_Proof	OT.Active_Auth_Proof	OT. AC_Pers	OT. Data_Integrity	OT. Data_Authenticity	OT. Data_Confidentiality	OT. Identification	OT. Prot_Abuse-Func	OT. Prot_Inf_Leak	OT.Tracing	OT. Prot_Phys-Tamper	OT. Prot_Malfunction
FAU_SAS.1				x				x					
FCS_CKM.1/DH_PACE					x	x	x						
FCS_CKM.1/CA	x	x		x	x	x	x						
FCS_CKM.1/CA_EC_KeyPair	x	x			x								
FCS_CKM.1/AA_EC_KeyPair	x		x		x								
FCS_CKM.4	x			x	x	x	x						
FCS_COP.1/CA_ENC	x	x		x	x		x						
FCS_COP.1/CA_MAC	x	x		x	x	x							
FCS_COP.1/PACE_ENC							x						
FCS_COP.1/PACE_MAC					x	x							
FCS_COP.1/SIG_VER	x			x									
FCS_COP.1/AA_SGEN_EC			x										
FCS_RND.1	x			x	x	x	x						
FIA_AFL.1/PACE											x		
FIA_UID.1/PACE	x			x	x	x	x						
FIA_UAU.1/PACE	x			x	x	x	x						
FIA_UAU.4/PACE	x			x	x	x	x						
FIA_UAU.5/PACE	x			x	x	x	x						
FIA_UAU.6/PACE					x	x	x						
FIA_UAU.6/EAC	x			x	x	x	x						
FIA_API.1/CA		x											
FIA_API.1/AA			x										
FDP_ACC.1/TRM	x			x	x		x						
FDP_ACF.1/TRM	x			x	x		x						
FDP_RIP.1					x	x	x						
FDP_UCT.1/TRM	x				x		x						
FDP_UIT.1/TRM					x		x						
FMT_SMF.1		x		x	x	x	x	x					
FMT_SMR.1/PACE		x		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												
FMT_MTD.1/CVCA_UPD	x												
FMT_MTD.1/DATE	x												
FMT_MTD.1/CA_AA_PK	x	x			x								

FMT_MTD.1/PA				x	x	x	x						
FMT_MTD.1/KEY_READ	x	x		x	x	x	x						
FMT_MTD.3	x												
FPT_EMS.1				x						x			
FPT_TST.1										x			x
FPT_FLS.1										x			x
FPT_PHP.3					x					x		x	
FTP_ITC.1/PACE					x	x	x				x		

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

The security objective **OT.AC_Pers** "Access Control for Personalization of logical travel document" addresses the access control of writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document.

FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing S.OD and, in generally, personalization data). The SFR FMT_SMR.1/PACE lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization).

The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Personalization Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE.

If the Personalization Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication).

If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1 or Active Authentication, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE 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/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication , of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{enc}). The SFR

FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER. The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA’s public key and certificate as well as the current date are written or updated by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA_EC_KeyPair is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [13] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Active_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Active Authentication Protocol provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FCS_CKM.1/AA_EC_KeyPair is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CA_AA_PK and FMT_MTD.1/KEY_READ. The key pair is generated using FCS_CKM.1/AA_EC_KeyPair. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/AA_SGEN_EC (for the generation of the digital signatures).

The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

The security objective **OT.Prot_Inf_Leak** “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the travel document’s chip against disclosure

- 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 which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document 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). This objective is achieved as follows:

i. while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
ii. for listening to PACE communication – FTP_ITC.1/PACE.

The security objective **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” is covered by the SFR FPT_PHP.3.

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by

i. the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and
ii. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

7.10.2 Dependency Rationale

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.

The following Table shows the dependencies between the SFR of the TOE

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, Fulfilled by FCS_CKM.4 from [2]
FCS_CKM.4 from [2]	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, FCS_CKM.1/CA_EC_KeyPair FCS_CKM.1/AA_EC_KeyPair
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4 from [2]

	key generation], FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4 from [2]
FCS_CKM.1/CA_EC_KeyPair	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC Fulfilled by FCS_CKM.4 from [2]
FCS_CKM.1/AA_EC_KeyPair	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/AA_SGEN_EC Fulfilled by FCS_CKM.4 from [2]
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4 from [2]
FCS_COP.1/AA_SGEN_EC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CA_EC_KeyPair, FCS_CKM.1/AA_EC_KeyPair Fulfilled by FCS_CKM.4 from [2]
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1/CA	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control,	Fulfilled by FDP_ACC.1/TRM, justification 1 for non-satisfied

	FMT_MSA.3 Static attribute initialization	dependencies
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [2] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [2] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [2] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CA_AA_PK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [2] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [2] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.

Justification for non-satisfied dependencies between the SFR for TOE:

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

No. 2: (i) Dependency "FCS_CKM.1 Cryptographic key generation" is not useful since all keys for Terminal Authentication are generated outside of the TOE, see "A.Auth_PKI PKI for Inspection Systems". (ii) Dependencies "FDP_ITC.1 Import of user data without security attributes" and "FDP_ITC.1 Import of user data with security attributes" are not necessary because all keys are written using SFR FMT_MTD.1/CVCA_INI.

7.10.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit 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 be economically feasible to retrofit to an existing product line. 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 sensitive security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the travel document’s development and manufacturing especially for the secure handling of the travel document’s material.

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.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The selection of the component ALC_FLR.1 provides basic handling of security flaws. This component provides guidance procedures on how to handle security flaws (i.e.: tracking, documentation, correction, status).

The selection of the component ALC_CMS.5 provides the highest available assurance level regarding the management of configuration items. The configuration lists contains configuration items such as the implementation representation, development tools and security flaws. This configuration items play an important role in the production of a quality TOE version and are important to maintain in a controlled manner.

The selection of the component ALC_TAT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring to document the TOE development tools.

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.2 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_TDS.3 Basic modular design
- ADV_FUN.1 Functional testing

All of these are met or exceeded in the EAL4 assurance package.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

All of these are met or exceeded in the EAL4 assurance package.

The component ALC_FLR.1 has no dependencies.

The component ALC_CMS.5 has no dependencies.

The component ALC_TAT.2 has the following dependencies: ADV_IMP.1 which is met by the EAL4 assurance package.

7.10.4 Security Requirements - Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

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

The dependency analysis in section *Dependency Rationale* Dependency Rationale 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-satisfied dependencies are appropriately explained.

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

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section *Security Assurance Requirements Rationale* shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections Dependency Rationale and Security Assurance Requirements Rationale. Furthermore, as also discussed in section Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

8 TOE summary specification (ASE_TSS)

This TOE provides the following Security Services:

- Identification and Authentication
- Access Control
- Cryptographic OperationsData Confidentiality
- Data Integrity
- Protection
- Application Data and Key Management

8.1 TOE Security Services

8.1.1 Identification and Authentication

This service provides identification and authentication of the following user roles:

1. Manufacturer (IC or travel document),
2. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System
8. Foreign Extended Inspection System

according to FMT_SMR.1/PACE.

Note: a user acting in the role of Travel Document Manufacturer or Personalization Agent acts in the role of the Administrator.

The TOE does not provide any security services or allows any actions by any subjects unless identified and authenticated except (FIA_UID.1/PACE, FIA_UAU.1/PACE):

1. to establish a communication channel,
2. carrying out the PACE Protocol according to [5],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol v.1 according to [13]
6. to carry out the Terminal Authentication Protocol v.1 according to [13]
7. to carry out the Active Authentication Protocol according to [5] [70].

Chip Authentication

This service allows to prove identity (FIA_API.1/CA) and authenticate the TOE's chip using the Chip Authentication Protocol Version 1 by using ECDH generated session keys (FCS_CKM.1/CA).

The TOE verifies that each command was sent by the Inspection System that was successfully authenticated using the Chip Authentication Protocol by verifying the MAC (FIA_UAU.5/PACE ,FIA_UAU.6/EAC, FCS_COP.1/CA_MAC). In case an error occurs (FPT_FLS.1) or a MAC cannot be verified the secure messaging session is aborted and the Inspection System must re-authenticate.

[70] [assignment: list of TSF-mediated actions]

Terminal Authentication
This service provides (FIA_UID.1/PACE, FIA_UAU.1/PACE) the Terminal Authentication Protocol v.1 according to [13] (FIA_UAU.5/PACE).

This service allows the TOE to authenticate a Terminal by verifying a signature (FCS_COP.1/SIG_VER) generated by the Terminal. On each new authentication attempt of the Terminal a new randomly generated challenge (FCS_RND.1) by the TOE must be signed by the Terminal to prevent replay attacks (FIA_UAU.4/PACE).

Active Authentication
This service allows to prove the TOE's identity (FIA_API.1/AA) using the Active Authentication Protocol according to [5] (FIA_UAU.5/PACE).

This services provides the ability to perform an authentication using the Active Authentication Protocol with EC keys that

- are generated off-card by the Personalization Agent or Manufacturer (FMT_MTD.1/CA_AA_PK) during Life-Cycle phase 2 or 3 or
- are generated on the chip.

The TOE generates ECDSA based digital signatures (FCS_COP.1/AA_SGEN_EC) in the process of an Active Authentication Protocol session.

Passive Authentication
This service provides the Passive Authentication according to [5] (FIA_UAU.5/PACE).

PACE Protocol Authentication
This service provides the PACE Protocol according to [5] (FIA_UAU.5/PACE).

On each new authentication attempt of the BIS-PACE a new randomly generated challenge (FCS_RND.1) by the TOE must be signed by the BIS-PACE to prevent replay attacks (FIA_UAU.4/PACE).

The TOE verifies that each command was sent by the Inspection System that was successfully authenticated using the PACE Protocol by verifying the MAC (FIA_UAU.5/PACE ,FIA_UAU.6/EAC, FCS_COP.1/CA_MAC). In case an error occurs (FPT_FLS.1) or a MAC cannot be verified the secure messaging session is aborted and the Inspection System must re-authenticate.

Symmetric Mutual Authentication
The TOE provides Device Authentication according to EN 419212-3 [42], Section 3.8 for Authentication of the Personalization Agent (FIA_UAU.5/PACE).

8.1.2 Access Control

This service provides access control to protect data from unauthorized disclosure (FDP_UCT.1/TRM, FDP_ACC.1/TRM).

After life-cycle personalization only terminals that can be successfully authenticated and authorized are allowed to read, write or modify data on the TOE (FDP_ACF.1/TRM).

Read Access
Only an Extended Inspection System that is authorized by the relative certificate holder und which certificate and certificate chain can be successfully verified by the TOE can read iris or fingerprint data (FDP_ACF.1/TRM).

Nobody can read intrinsic cryptographic keys that are stored on the TOE (FDP_ACF.1/TRM, FMT_MTD.1/KEY_READ).

This service only allows the Personalisation Agent to access the Initialisation Data and Pre-personalisation Data for reading (FMT_MTD.1/INI_DIS).

Write Access

The manufacturer in the role of the IC manufacturer writes the Initialisation Data (Keys to authenticate and optionally to establish a secure channel) during Life-Cycle phase 2 to the audit records (FAU_SAS.1, FMT_MTD.1/INI_ENA,)

The manufacturer in the role of the travel document manufacturer writes the Pre-Personalisation Data during Life-Cycle phase 2. The Pre-Personalisation Data allows the Personalisation Agent to authenticate to the TOE in Life Cycle phase 3 (FMT_MTD.1/INI_ENA).

8.1.3 Cryptographic Operations

This service provides a true random number generator (FCS_RND.1) to allow secure authentication using the PACE protocol according to [5].

This service provides signature verification (FCS_COP.1/SIG_VER) to allow terminal authentication using Terminal Authentication Protocol v.1 (FIA_UID.1.1/PACE, FIA_UAU.1/PACE):

8.1.4 Data Confidentiality

This service provides the Secure messaging in MAC-ENC mode according to [5] (FIA_UAU.5/PACE).

Secure Messaging

After successfully running the PACE protocol according to [5] this service provides an AES or TDES encrypted (FCS_COP.1/PACE_ENC) data stream between an authenticated entity and the TOE. The PACE protocol uses sessions keys agreed upon by using ECDH (FCS_CKM.1/DH_PACE).

After successfully running the Chip Authentication Protocol using EC keys (FCS_CKM.1/CA_EC_KeyPair) or the Active Authentication Protocol using EC keys (FCS_CKM.1/AA_EC_KeyPair) this service provides an AES or TDES encrypted (FCS_COP.1/CA_ENC) data stream between an authenticated entity and the TOE. The Chip Authentication Protocol uses sessions keys agreed upon by using ECDH (FCS_CKM.1/CA).

8.1.5 Data Integrity

Secure Messaging

This service provides protection from modification, deletion, insertion and replay of transmitted data and detects such (FDP_UIT.1/TRM, FTP_ITC.1/PACE).

This service provides the Secure messaging in MAC-ENC mode according to [5] (FIA_UAU.5/PACE).

After successfully running the PACE protocol according to [5] this service provides an integrity protected (FCS_COP.1/PACE_MAC) data stream using CMAC or Retail-MAC between an authenticated entity and the TOE. The PACE protocol uses sessions keys agreed upon by using ECDH (FCS_CKM.1/DH_PACE).

In case an error occurs during secure messaging communication, i.e. a command cannot be verified (FCS_COP.1/PACE_MAC) the session keys are destroyed (FCS_CKM.4).

After successfully running the Chip Authentication Protocol according to [13] this service provides an integrity protected (FCS_COP.1/CA_MAC) data stream using CMAC or Retail-MAC between an authenticated entity and the TOE. The Chip Authentication Protocol uses sessions keys agreed upon by using ECDH (FCS_CKM.1/CA).

In case an error occurs during secure messaging communication, i.e. a command cannot be verified (FCS_COP.1/CA_MAC) the session keys are destroyed (FCS_CKM.4).

After successfully running the Device Authentication protocol according to EN 419212-3 [42], Section 3.8 this service provides an integrity protected (FCS_COP.1/CA_MACFCS_COP.1/CA_MAC) data stream using CMAC or Retail-MAC between the (pre-) personalisation agent and the TOE.

Integrity Self Test

This service runs file system integrity self-test after reset on OS start-up .

This service also ensures that sensitive data stored on the TOE, in particular TSF and user data or keys used by the security functionality and any code are integrity protected. Data integrity is verified on any data access (FPT_TST.1).

This service ensures furthermore that only executable code is stored on the TOE which integrity is verified. The integrity of code is also verified during loading in life-cycle phase 1 and 2 (FPT_TST.1).

8.1.6 Protection

Hardware and Software (IC Security Embedded Software)

This service makes test features that are used in phases 1 – 3 unavailable in order to protect data to be disclosed or manipulated by unauthorized users or to gain knowledge about the TOE to facilitate attacks (FMT_LIM.1, FMT_LIM.2).

This service also ensures that the TOE always operates in a secure state (TOE reset or switching to life-cycle TERMINATED) even if an attack or failure is detected or operating conditions are causing a malfunction (FPT_FLS.1, FPT_PHP.3).

This service ensures that no variations in IC power consumption or electromagnetic emissions and variations in command execution time are emitted by the TOE to allow an attacker to gain sensitive data stored on the TOE that is used for identification, authentication and secure messaging purposes or to corrupt the security functionality of the TOE (software: FPT_EMS.1, hardware: FDP_ITT.1 and FPT_ITT.1).

Software (IC embedded software)

The service protects session key data and other ephemeral private keys by destroying it (FCS_CKM.4, FDP_RIP.1)

- after closing a secure messaging session
- on detection of an error during command execution

If the TOE detects 3 consecutive unsuccessful authentication/verification attempts using the

- PACE protocol according to [5]

a delay of 1 second will be in place for following authentication attempts (FIA_AFL.1/PACE). The delay increases exponentially with every further un-successful authentication attempt. Only after a successful authentication the delay is re-set to its default value.

8.1.7 Application Data and Key Management

This service provides the ability to initialize, configure and to perform pre-personalisation and personalisation of the TOE (FMT_SMF.1).

Only the manufacturer is allowed to write initialisation data and pre-personalisation data in life-cycle phase 2 to the TOE (FMT_MTD.1/INI_ENA).

This service restricts the ability to read initialisation data and pre-personalisation to the personalisation agent (FMT_MTD.1/INI_DIS).

This service allows the personalisation agent to write the document security object and restricts the write access in consecutive life cycles (FMT_MTD.1/PA).

This service allows the Manufacturer in life-cycle phase 2 or the Personalisation Agent in life-cycle phase 3 to write initial Country Verifying Certification Authority Public Key, initial Country Verifying Certification Authority Certificate, initial Current Date to the TOE (FMT_MTD.1/CVCA_INI) and restricts the write access in consecutive life cycles (FMT_MTD.1/PA).

This service allows the Personalisation Agent in life-cycle phase 3 to create or load the Chip Authentication Private Key and Active Authentication Private Key to Personalization Agent (FMT_MTD.1/CA_AA_PK) and restricts the write access in consecutive life cycles (FMT_MTD.1/PA).

This service restricts the ability to update the Country Verifying Certification Authority Public Key, Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority (FMT_MTD.1/CVCA_UPD).

This service restricts the ability to modify the Current date to Country Verifying Certification Authority, Document Verifier and Domestic Extended Inspection System (FMT_MTD.1/DATE).

This service ensures that only secure values for the certificate chain are accepted (FMT_MTD.3).

8.2 Statement of Compatibility

This section shows the compatibility of this Composite ST and the Platform-ST as required by [43].

The Platform-ST is the security target of Infineon Security Controller IFX_CCI_000005h H13 and IFX_CCI_000008h H13 used by this TOE as platform.

8.2.1 Security Assurance Requirements

The Hardware-Platform Security Target provides

- EAL6 augmented by ALC_FLR.1

The Composite-ST requires:

- EAL4 augmented with ALC_DVS.2, ATE_DPT.2, AVA_VAN.5, ALC_FLR.1, ALC_CMS.5 and ALC_TAT.2.

8.2.2 Assumptions

The following table list all assumptions of the hardware platform related to its operational environment not relevant for this ST.

Assumptions of the HW platform related to its operational environment inherited from [24]	Meaning	Operational Environment of this TOE
A.Plat-Appl	Usage of Hardware Platform	n.a.

The following table list all relevant assumptions of the hardware platform related to its operational environment which are fulfilled by the ST.

Assumptions of the HW platform related to its	Meaning	Operational Environment of this TOE

operational environment inherited from [24]		
A.Resp-Appl	Treatment of User Data	OT.Data_Integrity OT.Data_Authenticity OT.Prot_Abuse-Func OT.Prot_Phys-Tamper
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	OT.Identification

8.2.3 Security Objectives

The following table lists all security objectives of the hardware platform and mapped to the relevant security objective of this ST.

Security objectives of the Platform-ST	OTs of the Composite-ST									
	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Inf_Leak	OT.Prot_Abuse-Func	OT.Identification	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality
O.Phys-Manipulation	x									
O.Phys-Probing	x									
O.Malfunction	x	x								
O.Leak-Inherent			x							
O.Leak-Forced			x			x		x	x	x
O.Abuse-Func				x						
O.Identification					x					
O.RND						x		x	x	x
O.Add-Functions						x	x	x	x	x

The security objectives of the Platform-ST and the OTs of this Composite-ST are not contradictory since they can be mapped.

The following security objective of platform cannot be mapped to OTs of this ST

- O.Mem-Access

since no OT of the Composite-ST needs the respective security functionality.

For the following OTs of the Composite-ST no security objectives of platform exists

- OT.Sens_Data_Conf
- OT.Tracing
- OT.AC_Pers

since no security objectives of the Platform-ST provides a functionality needed by this TOE.

With the mapping of security objectives of platform and the security objectives of this ST all security objectives are listed and therefore the security objectives of the Platform-ST are not contradictory to those of this composite ST.

8.2.4 Security Objectives Environment

The Security Target of the Hardware Platform lists the following Security Objectives for the operational environment:

- OE.Lim_Block_Loader
- OE.TOE_Auth
- OE.Loader_Usage secure
- OE.Process-Sec-IC

According to the "Note 8", Page 53 of the Security Target these objectives only apply when the HW platform comes with an activated Flash Loader.

This is especially the case for "Option b)" in Life Cycle Phase 1 (see Chapter 2.4.4), which means that the Travel Document Manufacturer is enabled to download the Chip Embedded Software using the Loader provided by the Chip Dedicated software.

In this situation the Travel Document Manufacturer still act's as the "TOE Manufacturer" in the sense of the Chip Hardware Certification and therefore the Objectives for the Operational Environment as given in the Hardware Platform Security Target apply to him directly and therefore don't need to be re-stated in the Security Target at hand.

In the sense of ASE_COMP.1 these Objectives are rated as Ir.OE as they address the TOE Manufacturer in the sense of the Chip Hardware Certification.

Note: The IC Embedded Software to be loaded does not provide Loader Functionality itself.

Objective for the Operational Environment in the HW platform ST	Meaning	Classification	Operational Environment of this TOE
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	Ir.OE	n/a
OE.TOE_Auth	Authentication to external entities	Ir.OE	n/a
OE.Loader_Usage secure	communication and usage of the Loader	Ir.OE	n/a
OE.Process-Sec-IC	Protection during composite product manufacturing	Ir.OE	n/a

8.2.5 Organizational Security Policies

The Platform-ST lists two organizational security policies:

- P.Process-TOE
- P.Add-Functions.

OSP P.Process-TOE of the platform is relevant since this organizational security policy is covered by

- OSP P.Manufact

of the Composite-ST.

OSP P.Add-Functions of the platform is relevant since this policy provides security functionality needed by

- OT.Chip_Auth_Proof (ECDH)
- OT.Active_Auth_Proof (EC)
- OT.Data_Integrity (AES and TDES)
- OT.Data_Authenticity (AES and TDES)

The organizational security policies of the Platform-ST and the OTs of this Composite-ST are not contradictory since they are not relevant or can be used directly by this TOE.

8.2.6 Threats

The following table provides a mapping of the threats of the Platform-ST to the threats of this ST.

Threats of the Platform-ST	Threats of this ST							
	T.Phys-Tamper	T.Forgery	T.Malfunction	T.Information_Leakage	T.Abuse-Func	T.Counterfeit	T.Skimming	T.Eavesdropping
T.Leak-Inherent				x				
T.Phys-Probing	x	x						
T.Malfunction	x	x	x					
T.Phys-Manipulation	x	x						
T.Leak-Forced				x		x	x	x
T.Abuse-Func					x			
T.RND						x	x	x
T.Mem-Access	x		x		x			

8.2.7 Security Functional Requirements

The relevant security requirements of the composite TOE can be mapped directly to the hardware's SFRs. None of them show any conflicts between each other. Platform SFRs that are not used by the composite ST are not listed.

Platform SFR	Meaning	Category[71]	Supports TOE SFR
FRU_FLT.2	Limited Fault Tolerance	RP_SFR-MECH	FPT_TST.1
FPT_FLS.1	Failure with Preservation of Secure State	RP_SFR-MECH	FPT_FLS.1
FPT_PHP.3	Resistance to Physical Attack	RP_SFR-MECH	FPT_PHP.3
FDP_ITT.1	Basic Internal Transfer Protection	RP_SFR-MECH	FPT_EMS.1
FDP_IFC.1	Subset Information Flow	RP_SFR-MECH	FPT_EMS.1

[71] Either „IP_SFR“: irrelevant, „RP-SFR-SERV”: relevant in TSFI implementation, “RP_SFR-MECH”: relevant and addressed in ARC

	Control		
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	RP_SFR-MECH	FPT_EMS.1
FCS_RNG.1	Quality Metric for Random Numbers	RP-SFR-SERV	FCS_CKM.1/CA_EC_KeyPair, (EC Key Pair generation for CA) FCS_CKM.1/AA_EC_KeyPair (EC Key Pair generation for AA) FIA_UID.1/PACE for - (2) PACE Protocol - (5) Terminal Authentication Protocol v.1 FCS_CKM.1/CA FPT_EMS.1 (blinding) FCS_RND.1
FPT_TST.2	Subset TOE Security Testing	RP_SFR-MECH	FPT_TST.1 FPT_PHP.3
FCS_CKM.1/EC	Cryptographic key generation	RP-SFR-SERV	FCS_CKM.1/CA_EC_KeyPair, FCS_CKM.1/AA_EC_KeyPair
FCS_COP.1/ECDH	Cryptographic Support (ECDH)	RP-SFR-SERV	FCS_CKM.1/CA, FCS_CKM.1/DH_PACE
FCS_COP.1/ECDSA	Cryptographic Support (ECDSA)	RP-SFR-SERV	FCS_COP.1/SIG_VER FCS_COP.1/AA_SGEN_EC
FCS_COP.1/DES	Cryptographic Support (3DES)	RP-SFR-SERV	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC
FCS_COP.1/AES	Cryptographic Support (AES)	RP-SFR-SERV	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC
FAU_SAS.1	Audit Storage	RP-SFR-SERV	FAU_SAS.1
FMT_LIM.1	Limited Capabilities	RP_SFR-MECH	FMT_LIM.1
FMT_LIM.2	Limited Availability	RP_SFR-MECH	FMT_LIM.2
FDP_ACC.1	Subset Access Control	RP_SFR-MECH	FPT_FLS.1
FDP_ACF.1	Security Attribute Based Access Control	RP_SFR-MECH	FPT_FLS.1
FDP_SDI.1	Stored Data Integrity Monitoring	RP_SFR-MECH	FPT_PHP.3, not used by TSF directly
FDP_SDI.2	Stored Data Integrity Monitoring and Action	RP_SFR-MECH	FPT_PHP.3, not used by TSF directly
FMT_MSA.1	Management of Security Attributes	RP_SFR-MECH	FPT_EMS.1, FPT_FLS.1, FPT_PHP.3
FMT_MSA.3	Static Attribute Initialization	RP_SFR-MECH	FPT_EMS.1, FPT_FLS.1, FPT_PHP.3
FMT_SMF.1	Specification of Management Functions	RP_SFR-MECH	FPT_FLS.1, FPT_PHP.3

There is no conflict between the security problem definition, the security objectives and the security requirements of the composite ST and the platform ST. All related details (operations on SFRs, definition of security objectives, threats) can be found in both STs.

9 Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [5].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [4], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
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.
Active Authentication	Security mechanism defined in [6] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
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 travel document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organisation
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys
Basic Inspection System with PACE protocol (BIS- PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographic data (biodata).	The personalised details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [6]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.

Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [6]
Country Signing CA Certificate (C CSCA)	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [6], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [5]
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (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 terminals using it 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 [5]. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [5].
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Card Verifiable Certificate according to [5].
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [6] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [4],
Document Details Data	Data printed on and electronically stored in the travel document 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 travel document's chip. It may carry the Document Signer Certificate (C DS). [6]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [5]and [6] This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) 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 Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [5]. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip
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. [6]
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
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 [5].
Extended Access Control	Security mechanism identified in [6] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organisation to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [6]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is

	a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel documents. [6]
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 Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
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.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
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. [6]
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. [6]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document’s material (IC identification data).
Inspection	The act of a State examining an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [6]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document’s chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document’s chip have not been altered from that created by the issuing State or Organisation
Issuing Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [6]
Issuing State	The Country issuing the travel document. [6]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the travel document’s chip

Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [6] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) personal data of the travel document holder the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), the digitized portraits (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and the other data according to LDS (EF.DG5 to EF.DG16). EF.COM and EF.SOD
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. [6]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [6] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
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. [6]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [5]. The metadata of a CV certificate comprise the following elements: Certificate Profile Identifier, Certificate Authority Reference, Certificate Holder Reference, Certificate Holder Authorisation Template, Certificate Effective Date, Certificate Expiration Date
ePassport application	Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes the file structure implementing the LDS [6], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [4],. 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.
PACE Password	A password needed for PACE authentication, e.g. CAN or MRZ.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the “Enrolment” (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: establishing the identity of the travel document holder for the biographic data in the travel document, enrolling the biometric reference data of the travel document holder, writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [5], writing the document details data, writing the initial TSF data, signing the Document Security Object defined in [6] (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 travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role
Personalisation Data	A set of data incl. individual-related data (biographic and biometric data) of the travel document holder, dedicated document details data and dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document’s chip to verify the authentication attempt of a terminal as Personalisation Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) biographical data, data of the machine-readable zone, photographic image and other data
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document’s and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair.
Pre-personalised travel document’s chip	travel document’s chip equipped with a unique identifier.

Receiving State	The Country to which the traveller is applying for entry. [6]
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.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [15].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [6]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [14]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [4], namely (i) PACE or BAC and (ii) Passive Authentication with SO D . SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	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 [6] (there "Machine readable travel document").
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [6], sec III.

Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
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	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [6]
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.

10 Acronyms

Acronym	Term
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
EAC	Extended Access Control
EF	Elementary File
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Personalisation Terminal
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)

11 Bibliography

[1] *BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile / Machine ReadableTravelDocumentwith 'ICAOApplication', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05..*

[2] *Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22nd July 2014.*

[3] *REGULATION (EC) No 444/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 28 May 2009..*

[4] *REGULATION (EU) 2017/1954 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, 25 October 2017..*

[5] *International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Part 11: Security Mechanisms for eMRTDs", seventh edition, 2015.*

[6] *ISO/IEC 7816-3 Identification cards - Integrated circuit - Cards with contacts - Electrical interface and transmission protocols, Third edition 2006-11-01.*

[7] *ISO/IEC 7816-4 "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange", third edition 2013-04-15.*

[8] *ISO/IEC 7816-8 "Identification cards - Integrated circuit cards - Part 8: Commands and mechanisms for security operations", third edition 2016-11-01.*

[9] *ISO/IEC 7816-9 "Identification cards - Integrated circuit cards - Part 9: Commands for card management", 2017, third edition 2017-12.*

[10] *ISO/IEC 14443-1:2018 Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics.*

[11] *ISO/IEC 14443-2:2016, Identification cards - Contactless integrated circuit, cards - Proximity cards - Part 2: Radio frequency power and signal interface.*

[12] *ISO/IEC 14443-3:2018, Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision.*

[13] *Technical Guideline TR-03110 Part 1-4, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token.*

[14] *Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste.*

[15] *Infineon, Common Criteria Public Security Target, EAL6 augmented / EAL6+, IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h H13.*

[16] *Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014..*

[17] BSI, "Certification Report BSI-DSZ-CC-1110-V4-2021," 2021.

[18] *International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010.*

[19] *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.*

[20] *Security Target - ACOS-IDv2.0 eMRTD (B) BAC configuration.*

[21] *ISO/IEC 18013-1:2018 Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set.*

[22] *ISO/IEC TR 19446:2015 Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications.*

[23] *COMMISSION REGULATION (EU) No 383/2012 aying down technical requirements with regard to driving licences which include a storage medium, of 4 May 2012.*

[24] *Eurosmart Security IC Platform Protection Profile with Augmentation Packages, registered under BSI-CC-PP-0084-2014, Version 1.0, dated 2014-01-13.*

[25] *Austria Card, Preparation and Operational Manual - ACOS-IDv2.0 eMRTD, BAC and PACE/EAC configuration, Version 1.04, Date 2021-11-29.*

[26] *Austria Card, ACOS-ID User Manual, Version 2.12, Date 19.05.2021.*

[27] *Internal Operation Manual - ACOS-IDv2.0, Version 1.2, 2021-07-19.*

[28] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.*

[29] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, July 2017.*

[30] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, July 2017.*

[31] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017.*

[32] *Common Criteria Public Security Target, IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h.*

[33] *ISO/IEC 11770-3: Information technology — Security techniques — Key management -- Part 3: Mechanisms using asymmetric techniques, 2008.*

[34] *Technical Guideline BSI TR-03111, Elliptic Curve Cryptography, Version 2.10, 2018.*

[35] BSI-TR-03111, *Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111, Version 1.11, 17.04.2009.*

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

[37] *BSI, Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik.*

[38] *ISO/IEC 10116:2006 – Information technology – Security techniques – Modes of operation for an n-bit block cipher. 2006..*

[39] *ISO/IEC. ISO/IEC 18033-3:2010 – Information technology – Security techniques – Encryption Algorithms – Part 3: Block ciphers. 2010..*

[40] *FIPS 197, Advanced Encryption Standard (AES), NIST 2001.*

[41] *ISO/IEC, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011.*

[42] *EN 419212-3 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part-3.*

[43] *BSI, Anwendungshinweise und Interpretationen zum Schema, AIS36: Kompositionsevaluierung, Version 4, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik.*

[44] N. S. G. G. S. Infineon Technologies AG, *Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 2014.*

[45] *NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, December 2001.*

[46] S. T. -. A.-I. e. v. BAC.

[47] *ISO/IEC 14443-4:2018, Cards and security devices for personal identification - Contactless proximity objects - Part 4: Transmission protocol.*