Security Target-
ACOS-IDv4.1 eMRTD (A) BAC Configuration

Document Information

Author:	Thomas Aichinger
Title:	Security Target
Version:	1.27 public
Date:	2024-10-14
Company:	AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Lamezanstraße 4-8, 1230 Vienna, Austria
Classification:	Public

Document History

Version	Date	Author	Changes
v1.27 public	2024-10-14	AC	Public Version derived

1 Contents

[Intentionally blank]

2 Security Target Introduction (ASE_INT)

2.1 ST Reference

Title	Security Target - ACOS-IDv4.1 eMRTD (A) BAC Configuration
Version	1.27 public
Author	Austria Card Ges.m.b.H.
Compliant to	Common Criteria Protection Profile – Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC PP [1])
CC Version	3.1 Revision 5
Certification ID ANSSI	ACOS-ID
Assurance Level	EAL4+
Keywords	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Basic Access Control (BAC)

2.2 TOE Reference

TOE Name	ACOS-IDv4.1 eMRTD (A) BAC 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_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11, BSI-DSZ-CC-1229-V2-2024
TOE Version	v4.1 eMRTD (A)

2.3 TOE Overview

This Security Target defines the security objectives and requirements for the contact based / contactless chip of electronic documents (i.e. machine readable travel documents – MRTD, driving license) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the security methods Basic Access Control in the 'ICAO Doc 9303' [2] **and additionally Active Authentication according to** [2]**.**

ACOS-IDv4.1 eMRTD (A) BAC Configuration is a chip operating system compliant to ISO 7816-3 [3], ISO 7816-4 [4], ISO 7816-8 [5], ISO 7816-9 [6], ISO 14443 [7] [8] [9], BSI TR-03110 [10] and EN 419212 [11] 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_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 including software packages [12].

The secure chip and software packages (e.g. libraries) are certified according to CC EAL 6+ (see [13] for the latest certificate) according to the Protection Profile BSI-CC-PP-0084-2014 [14].

The TOE is a composition of ACOS-IDv4.1 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 based passport or smart card programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [2] **and additionally Active Authentication according to** [2]**.**

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

The TOE comprises at least

- the circuitry of the travel document's chip (the integrated circuit, IC)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the travel document application and
- the associated guidance documentation.

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

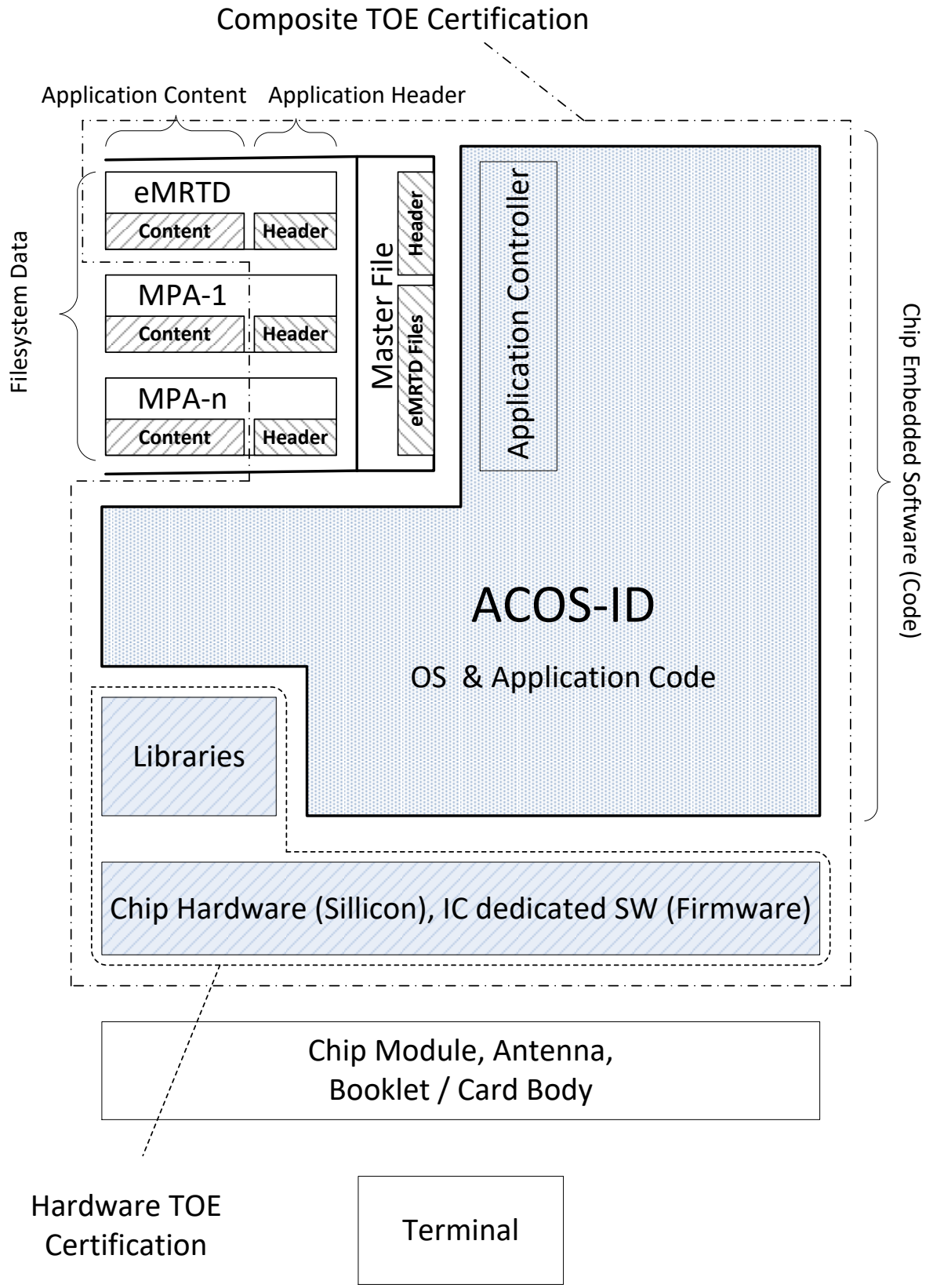


Figure 1 TOE Block Diagram

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 Organization issues travel documents to be used by the holder for international travel. The traveler presents a travel document to the inspection system to prove his or her identity. The travel document in context of this protection profile 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 according to LDS for contactless machine reading.

The authentication of the traveler is based on

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

The issuing State or Organization ensures the authenticity of the data of genuine travel document's. The receiving State trusts a genuine travel document of an issuing State or Organization.

For this Security Target the travel document is viewed as unit of

a) the **physical travel document** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
    1) the biographical data on the biographical data page of the passport book,
    2) the printed data in the Machine-Readable Zone (MRZ) and
    3) the printed portrait.

b) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure [2] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the travel document holder
    1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
    2) the digitized portraits (EF.DG2),
    3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]
    4) the other data according to LDS (EF.DG5 to EF.DG16) and
    5) the Document Security Object.

The issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The travel document as the passport book and the travel document's chip is uniquely identified by the Document Number.

The physical travel document is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the travel document's chip) and organizational security measures (e.g. control of materials, personalization procedures) [2]. These security measures include the binding of the travel document's chip to the passport book.

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 Organization 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 additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [2] as well as PACE / SAC. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This Security Target addresses the protection of the logical travel document

i. in integrity by write-only-once access control and by physical means, and

[1] These additional biometric reference data are optional.

ii. in confidentiality by the Basic Access Control Mechanism.

This Security Target **does address the Active Authentication** but not the Extended Access Control as optional security mechanisms.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system

i. reads optically the travel document,
ii. authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the travel document's chip provides read access to the logical travel document by means of private communication (secure messaging) with this inspection system [2], normative appendix 5.

EAC and PACE / SAC are additionally supported by the composite product, but it are not in the scope of this ST due to the fact that this security target only considers extended basic attack potential to the Basic Access Control Mechanism and Active Authentication (i.e. AVA_VAN.3) where EAC and PAC/SAC consider high attack potential (i.e. AVA_VAN.5). Therefore a separate evaluation and certification process using an ST [15] conformant to [16] is carried out contemporaneous to the current process.

The TOE can also be used as a driving license (IDL or eDL) compliant to ISO/IEC 18013 [17] or ISO/IEC TR 19446 [18] (according Commission Regulation (EU) No 383/2012 [19]) supporting BAC and AA 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 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 BAC 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 [16] 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 Reference: NSCIB SS-22-0575112)
- 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. [14]) to load the IC Embedded Software. The IC Security Target [14] addresses this topic in “P.Lim_Block_Loader” and “P.Ctrl_Loader”. See also [14] 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

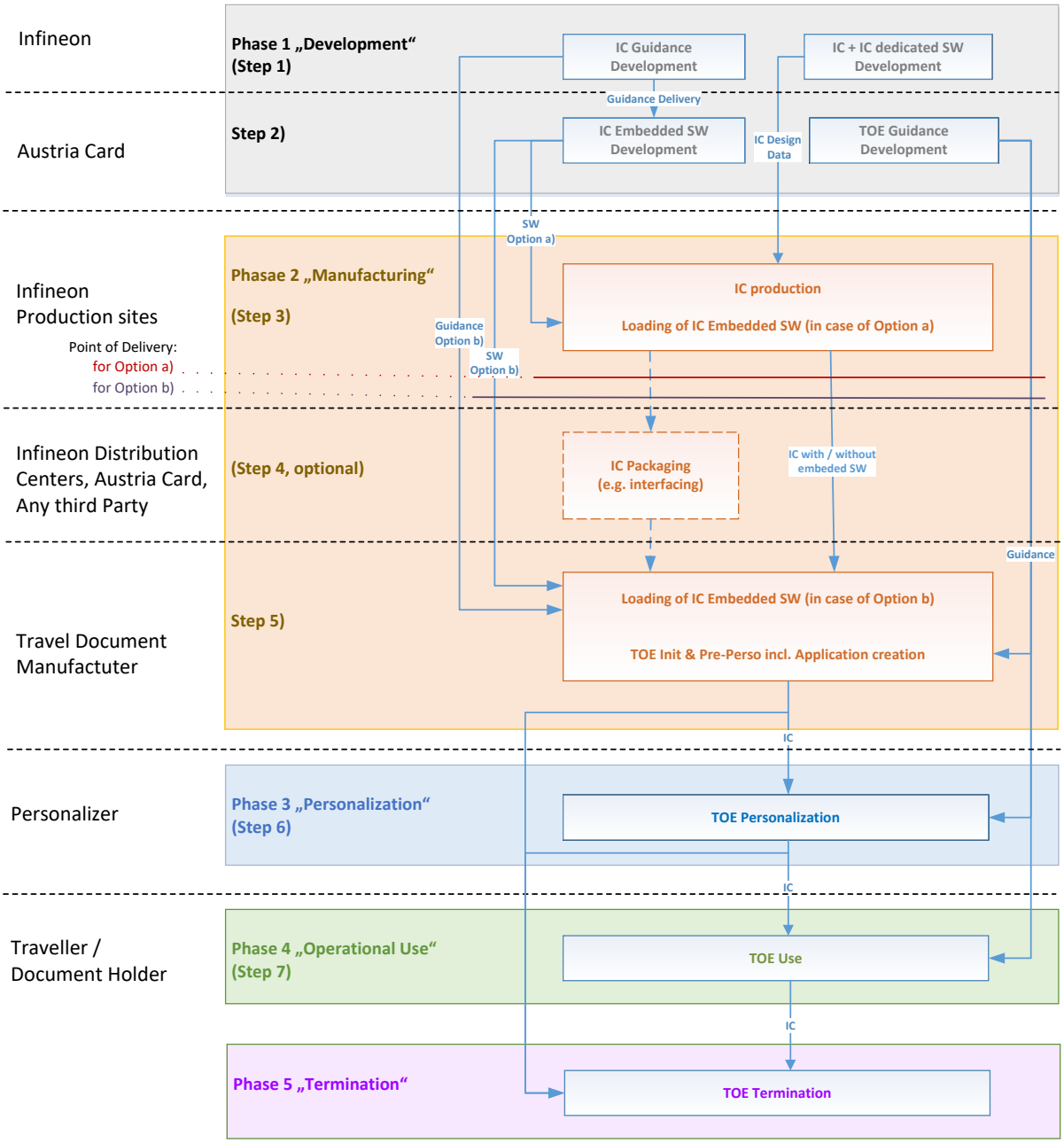
in Case of Option b)

- 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 [16] (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.



Phase 1 “Development”

(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[2] 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

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

(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),
(ii) creates the ePassport application (create the MF and ICAO.DF[3]), 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 [20] 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.

[3] See Application Note 1 of [16]

The TSF data[4] (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[5] 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 [2]. This approach allows but does not enforce the separation of these roles.

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[6].

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 2 from PP56v2

[5] See also Application Note 3 from PP56v2

[6] See also Application Note 4 from [16]

2.4.6 TOE Components

The TOE consists of the following components:

Category	**Definition**	**Format; Delivery Method**
Secure Chip Hardware	Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11	Hardware (wafer, module, smartcard, passport); physical delivery
Secure Chip Firmware	80.506.04.1	Software; included in "Secure Chip Hardware"
Secure Chip Vendor Software Libraries	CS-SLC26V19 CryptoSuite: v4.08.001 Hardware Support Layer (HSL): 04.05.0030 RFAPI: 40.00.2500 UMSLC: 02.01.0040	Software; included in "Operating System"
Operating System	ACOS-IDv4.1 Builds: 0x9486, 0x3C76, 0x2CE8 and 0x304F Those builds differ in their support of different configurations and features (availability of RSA, PACE protocols). The builds and the underlying code are represented by the label "REL_ACOS-IDv4.1_01" in the repository. This chip embedded software version corresponds to the Version Identifier "v4.1" of the TOE (part of the TOE name).	Software; for "Delivery Option a)" [7] included in "Secure Chip Hardware" for "Delivery Option b)" [8] electronic delivery via secured e-mail
Guidance Documentation	The Guidance consists of the following documents: • "Preparation and Operational Manual - ACOS-IDv4.1 eMRTD, BAC and EAC/PACE Configuration", Version 3.45, Date 2024-09-24 [21], • "User Manual", 4.05, Date 20.09.2024 [22], • "Internal Operation Manual", Version 2.1, 2024-04-11 [23] (only used Austria Card internal) Those documents are represented by the label "REL_ACOS-IDv4.1_eMRTD_CC-DOC_01" in the repository. This documentation version is reflected by the text "eMRTD (A)" part of the TOE name, where "eMRTD" refers to documentation for a specific type of certification and "(A)" to the specific version of the documentation.	Documents (pdf, scripts); electronic delivery via secured e-mail

[7] See chapter 2.4.4 for delivery options

[8] See chapter 2.4.4 for delivery options

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This ST claims conformance to the Common Criteria version 3.1 Revision 5, [24] [25] [26] as follows:

Part 2 extended due to the use of

- FIA_API.1
- FAU_SAS.1
- FCS_RND.1
- FMT_LIM.1
- FMT_LIM.2
- FPT_EMSEC.1

from 2009 [1],

Part 3 conformant.

For the evaluation the following methodology is used: [27].

3.2 PP Claim

This Security Target claims strict conformance to the Protection Profile:

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 [1].

3.3 Package claim

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

- ADV_FSP.5
- ADV_INT.2
- ADV_TDS.4
- ALC_CMS.5
- ALC_DVS.2
- ALC_FLR.1
- ALC_TAT.2
- ATE_DPT.3

as defined in CC part 3 [26].

3.4 Conformance Claim Rationale

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

> 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 [1].

The Security Problem Definition including Security Objectives and Threats from the underlying PP [1] have been taken as a whole to this Security Target and additional threats (see 4.5.1) and objectives (OT.Active_Auth_Proof, see 5.1.1) have been added.

Active Authentication is a challenge-response protocol defined in [2]:

- 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 by using an additional dedicated private key on the chip.

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 Extended Component Definition FIA_API has been added due to Active Authentication functionality.

Apart from the threats of the PP the threat **T.Counterfeit** has been added to this Security Target. This threat is mitigated by **OT.Active_Auth_Proof** and **OE.AA_Key_Travel_Document** which have been added to this Security Target**.**

OT.Active_Auth_Proof and OE.AA_Key_Travel_Document which are not in the original scope of the claimed PP [1] and have been added for the optional Active Authentication protocol mechanism. These objectives are only linked to threats for the Active Authentication protocol so they neither mitigate a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the underlying PP [1], nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the [1].

Active Authentication is a challenge-response protocol defined in [2]:

- the terminal sends a challenge (nonce) to the chip
- the chip 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.

In this ST the acronym “MRTD” has been replaced by the term “travel document”.

Conclusion:

3. The Threat added to the content of underlying PPs in this ST does not change the statement of Threats of the PP
4. The Security Objectives added to the content of underlying PPs in this ST do not change the statement of Security Objectives of the PP
5. The statement of Security Objectives in this ST remains consistent with the statement of Security Objectives in the PP.

4 Security Problem Definition (ASE_SPD)

4.1 Introduction

This ST introduces additional functionality Active Authentication which is not covered by the underlying Protection Profile [1]. Therefor some parts have been added in this section to amend the PP [1].

4.2 Assets

The assets to be protected by the TOE include the User Data on the travel document's chip.

Logical travel document Data

The logical travel document data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [2]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the travel document holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical travel document.

Due to interoperability reasons as the 'ICAO Doc 9303' [2] the TOE described in this Security Target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical travel document standard User Data (i.e. Personal Data) of the travel document holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4)[9]

A sensitive asset is the following more general one:

Authenticity of the travel document's chip

The authenticity of the travel document's chip personalized by the issuing State or Organization for the travel document holder is used by the traveler to prove his possession of a genuine travel document.

4.3 Subjects

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

[9] Cf. [25] for details how to access these User data under EAC protection.

	itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
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 these data on the physical and logical travel document for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data, (v) signing the Document Security Object defined in [2]. Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface.
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. The **Basic Inspection System** (BIS) i. contains a terminal for the contactless communication with the travel document's chip, ii. implements the terminals part of the Basic Access Control Mechanism and iii. gets the authorization to read the logical travel document under the Basic Access Control by optical reading the travel document or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System i. implements the Terminal Authentication Protocol and

	ii. is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates. Note: This protection profile does not distinguish between the BIS, GIS and EIS because the Extended Access Control is outside the scope.
Travel document holder	The rightful holder of the travel document for whom the issuing State or Organization personalized the travel document.
Traveler	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
Attacker	A threat agent trying i. to identify and to trace the movement of the travel document's chip remotely (i.e. without knowing or optically reading the printed MRZ data), ii. to read or to manipulate the logical travel document without authorization, or iii. to forge a genuine travel document. Note: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

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.

A.MRTD_Manufact	**Travel document manufacturing on steps 4 to 6**
It is assumed that appropriate functionality testing of the travel document is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the travel document and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).	

A.MRTD_Delivery	**Travel document delivery during steps 4 to 6**
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives: - Procedures shall ensure protection of TOE material/information under delivery and storage. - Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage. - Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.	

A.Pers_Agent	Personalization of the travel document's chip
The Personalization Agent ensures the correctness of i. the logical travel document with respect to the travel document holder, ii. the Document Basic Access Keys, iii. the Chip Authentication Public Key (EF.DG14) if stored on the travel document's chip, iv. the Document Signer Public Key Certificate (if stored on the travel document's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.	

A.Insp_Sys	Inspection Systems for global interoperability
The Inspection System is used by the border control officer of the receiving State (i) examining a travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2]. The Basic Inspection System reads the logical travel document under Basic Access Control and performs the Passive Authentication to verify the logical travel document.	

A.BAC-Keys	Cryptographic quality of Basic Access Control Keys
The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [2], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.	

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 threats are taken from the underlying Protection Profile [1].

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

T.Chip_ID	Identification of MRTD's chip
Adverse action:	An attacker trying to trace the movement of the travel document by identifying remotely the travel document's chip by establishing or listening to communications through the contactless communication interface.
Threat agent:	having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the travel document data page in advance
Asset:	Anonymity of user

T.Skimming	**Skimming the logical travel document**
Adverse action:	An attacker imitates an inspection system trying to establish a communication to read the logical travel document or parts of it via the contactless communication channel of the TOE.
Threat agent:	having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the travel document data page in advance
Asset:	confidentiality of logical travel document data

T.Eavesdropping	**Eavesdropping to the communication between TOE and inspection system**
Adverse action:	An attacker is listening to an existing communication between the travel document's chip and an inspection system to gain the logical travel document or parts of it. The inspection system uses the MRZ data printed on the travel document data page but the attacker does not know these data in advance.
Threat agent:	having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the travel document data page in advance
Asset:	confidentiality of logical travel document data

T.Forgery	**Forgery of data on travel document's chip**
Adverse action:	An attacker alters fraudulently the complete stored logical travel document or any part of it including its security related data in order to deceive on an inspection system by means of the changed travel document holder's identity or biometric reference data. This threat comprises several attack scenarios of travel document forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical travel document s to create a new forged travel document, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical travel document of a traveler into another travel document's chip leaving their digital MRZ unchanged to claim the identity of the holder this travel document. The attacker may also copy the complete unchanged logical travel document to another contactless chip.
Threat agent:	having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the travel document data page in advance
Asset:	authenticity of logical travel document data

T.Abuse-Func	**Abuse of Functionality**
Adverse action:	An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order i. to manipulate User Data, ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or iii. to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to travel document holder.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate travel document
Asset:	confidentiality and authenticity of logical travel document and TSF data, correctness of TSF

T.Information_Leakage	**Information Leakage from travel document's chip**
Adverse action:	An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate travel document
Asset:	confidentiality of logical travel document and TSF data

T.Phys-Tamper	**Physical Tampering**
Adverse action:	An attacker may perform physical probing of the travel document's chip in order i. to disclose TSF Data or ii. to disclose/reconstruct the travel document's chip Embedded Software. An attacker may physically modify the travel document's chip in order to i. modify security features or functions of the travel document's chip, ii. modify security functions of the travel document's chip Embedded Software, iii. modify User Data or iv. to modify TSF data.

	The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the travel document's chip) 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 direct interaction with the travel document's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and 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.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate travel document
Asset:	confidentiality and authenticity of logical travel document and TSF data, correctness of TSF

T.Malfunction	**Malfunction due to Environmental Stress**
Adverse action:	An attacker may cause a malfunction of TSF or of the travel document's chip Embedded Software by applying environmental stress in order to i. deactivate or modify security features or functions of the TOE or ii. circumvent, deactivate or modify security functions of the travel document's chip Embedded Software. This may be achieved e.g. by operating the travel document's chip outside the normal operating conditions, exploiting errors in the travel document's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate travel document
Asset:	confidentiality and authenticity of logical travel document and TSF data, correctness of TSF

4.5.1 Additional Threat (Active Authentication)

T.Counterfeit	**Counterfeit of travel document chip data**
Adverse action:	An attacker enhanced basic 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 enhanced basic attack potential, being in possession of one or more legitimate travel documents.

Asset:	authenticity of user data stored on the TOE and the authenticity of the chip itself.

4.6 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

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-personalization Data which contains at least the Personalization Agent Key.	

P.Personalization	**Personalization of the MRTD 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.Personal_Data	**Personal data protection policy**
The biographical data and their summary printed in the MRZ and stored on the travel document's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[10] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the travel document's chip are personal data of the travel document holder. These data groups are intended to be used only with agreement of the travel document holder by inspection systems to which the travel document is presented. The travel document's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [2].	

[10] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this Protection Profile.

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

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE. The listed Security Objectives are taken from the underlying Protection Profile [1].

OT.AC_Pers	**Access Control for Personalization of logical travel document**
The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document security object according to LDS [2] 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 its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.	
Note: 1) the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization 2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the “Operational Use” phase is optional.	

OT.Data_Int	**Integrity of personal data**
The TOE must ensure the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical travel document data.	

OT.Data_Conf	**Confidentiality of personal data**
The TOE must ensure the confidentiality of the logical travel document data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Basic Inspection System.	
Note: The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the travel document. The travel document’s chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data’s entropy. Any	

attack based on decision of the 'ICAO Doc 9303' [2] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification	**Identification and Authentication of the TOE**
The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the travel document". The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.	
Note: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the travel document". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or travel document identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.	

The following TOE security objectives address the protection provided by the travel document's chip independent of the TOE environment.

OT.Prot_Abuse-Func	**Protection against Abuse of Functionality**
After delivery of the TOE to the travel document Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.	
Note: Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.	

OT.Prot_Inf_Leak	**Protection against Information Leakage**
The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the travel document's chip • 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 and • 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. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper	**Protection against Physical Tampering**
The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the travel document's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of • measuring through galvanic contacts which is direct physical probing on the chips 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 charges (using tools used in solid-state physics research and IC failure analysis) • manipulation of the hardware and its security features, 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 functions.	

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 has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.	
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 objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.	

5.1.1 Additional Security Objectives (Active Authentication)

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 [2]. The authenticity proof provided by travel document's chip shall be protected against attacks with enhanced basic attack potential.[11]	

5.2 Security Objectives for the Operational Environment

5.2.1 Issuing State or Organization

The issuing State or Organization will implement the following security objectives of the TOE environment.

OE.MRTD_Manufact	**Protection of the MRTD Manufacturing**

[11] REFINEMENT

Appropriate functionality testing of the TOE shall be used in step 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_ Delivery	**Protection of the MRTD delivery**
Procedures shall ensure protection of TOE material/information under delivery including the following objectives: - non-disclosure of any security relevant information, - identification of the element under delivery, - meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment), - physical protection to prevent external damage, - secure storage and handling procedures (including rejected TOE's), - traceability of TOE during delivery including the following parameters: o origin and shipment details, o reception, reception acknowledgement, o location material/information. Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process. Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.	

OE.Personalization	**Personalization of logical travel document**
The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization i. establish the correct identity of the holder and create biographical data for the travel document, ii. enroll the biometric reference data of the travel document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and iii. personalize the travel document for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.	

OE.Pass_Auth_Sign	**Authentication of logical travel document by Signature**
The issuing State or Organization must i. generate a cryptographic secure Country Signing CA Key Pair, ii. ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and iii. distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine travel document in a secure operational environment only and	

(iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [2].

OE.BAC-Keys	**Cryptographic quality of Basic Access Control Keys**
The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [2] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.	

Additional SO for the OE (Active Authentication)

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 (i) generate the travel document's **Active Authentication Key Pair**, (ii) sign and store the **Active Authentication Public Key** data in **EF.DG15** and (iii) 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.	

5.2.2 Receiving State or Organization

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

OE.Exam_MRTD	**Examination of the travel document passport book**
The inspection system of the receiving State or Organization must examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [2].	

OE.Passive_Auth_Verif	**Verification by Passive Authentication**
The border control officer of the receiving State uses the inspection system to verify the traveler as travel document holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical travel document before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.	

OE.Prot_Logical_MRTD	**Protection of data from the logical travel document**
The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical travel document. The receiving State examining the logical travel document being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).	

5.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	**OT.Active_Auth_Proof**	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	**OE.AA_Key_Travel_Document**
T.Chip-ID				x										x				
T.Skimming			x											x				
T.Eavesdropping			x															
T.Forgery	x	x					x						x		x	x		
T.Abuse-Func					x							x						
T.Information_Leakage						x												
T.Phys-Tamper							x											
T.Malfunction								x										
T.Counterfeit									x									x
P.Manufact				x														
P.Personalization	x			x								x						
P.Personal_Data		x	x															
A.MRTD_Manufact										x								
A.MRTD_Delivery											x							
A.Pers_Agent												x						
A.Insp_Sys															x		x	
A.BAC-Keys														x				

The OSP **P.Manufact** “Manufacturing of the travel document’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.

The OSP **P.Personalization** “Personalization of the travel document by issuing State or Organization only” addresses the (i) the enrolment of the logical travel document by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization 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 Personalization of logical travel document”. Note the manufacturer equips the TOE with the Personalization 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 management of TSF to the Personalization Agent.

The OSP **P.Personal_Data** “Personal data protection policy” requires the TOE (i) to support the protection of the confidentiality of the logical travel document by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** “Integrity of personal data” describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** “Confidentiality of personal data” describes the protection of the confidentiality.

The threat **T.Chip_ID** “Identification of travel document’s chip” addresses the trace of the travel document movement by identifying remotely the travel document’s chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” and **T.Eavesdropping** “Eavesdropping to the communication between TOE and inspection system” address the reading of the logical travel document trough the contactless interface or listening the communication between the travel document’s chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** “Confidentiality of personal data” through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Forgery** “Forgery of data on travel document’s chip” addresses the fraudulent alteration of the complete stored logical travel document or any part of it. The security objective **OT.AC_Pers** “Access Control for Personalization of logical travel document “ requires the TOE to limit the write access for the logical travel document to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical travel document according the security objective **OT.Data_Int** “Integrity of personal data” and **OT.Prot_Phys-Tamper** “Protection against Physical Tampering”. The examination of the presented travel document passport book according to **OE.Exam_MRTD** “Examination of the travel document passport book” shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical travel document. The TOE environment will detect partly forged logical travel document data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** “Authentication of logical travel document by Signature” and verified by the inspection system according to **OE.Passive_Auth_Verif** “Verification by Passive Authentication”.

The threat **T.Abuse-Func** “Abuse of Functionality” addresses attacks using the travel document’s chip as production material for the travel document and misuse of the functions for personalization in the operational state after delivery to travel document holder to disclose or to manipulate the logical travel document. This threat is countered by **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality”. Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** “Personalization of logical travel document” ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to travel document holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage** “Information Leakage from travel document’s chip”, **T.Phys-Tamper** “Physical Tampering” and **T.Malfunction** “Malfunction due to Environmental Stress” are typical for integrated circuits like smart cards under direct attack with enhanced basic attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** “Protection against Information Leakage”, **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” and **OT.Prot_Malfunction** “Protection against Malfunctions”.

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.Active_Auth_Proof** “Proof of travel document’s chip authenticity” 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 assumption **A.MRTD_Manufact** “Travel document manufacturing on step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Manufact** “Protection of the travel document Manufacturing” that requires to use security procedures during all manufacturing steps.

The assumption **A.MRTD_Delivery** “Travel document delivery during step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_ Delivery** “Protection of the travel document delivery” that requires to use security procedures during delivery steps of the travel document.

The assumption **A.Pers_Agent** “Personalization of the travel document’s chip” is covered by the security objective for the TOE environment **OE.Personalization** “Personalization of logical travel document” including the enrolment, the protection with digital signature and the storage of the travel document holder personal data.

The examination of the travel document passport book addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objectives for the TOE environment **OE.Exam_MRTD** “Examination of the travel document passport book”. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** “Protection of data from the logical travel document” will require the Basic Inspection System to implement the Basic Access Control and to protect the logical travel document data during the transmission and the internal handling.

The assumption **A.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” is directly covered by the security objective for the TOE environment **OE.BAC-Keys** “Cryptographic quality of Basic Access Control Keys” ensuring the sufficient key quality to be provided by the issuing State or Organization.

6 Extended Component Definition (ASE_ECD)

This Security Target and its underlying protection profile [1] use components defined as extensions to CC part 2. Some of these components are defined in [28], other components are defined in this security target.

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 define the security functional requirements of the TOE a sensitive 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.

The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_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 dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: authorised users] with the capability to store [assignment: list of audit information] in the audit records

6.3 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive 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 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 the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

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

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family 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 the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

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*].

The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

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 test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase. The combination of both the requirements shall enforce the policy.	

6.5 Definition of the Family FPT_EMSEC

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks

against the TOE and other secret data 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 which are not directly addressed by any other component of CC part 2 [25].

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

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

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_EMSEC.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

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 [24] 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.

The operations “write”, “read”, “modify”, and “disable read access” are used in accordance with the general linguistic usage. The operations “transmit”, “receive” and “authenticate” are originally taken from [25].

7.1 Definitions

7.1.1 Subjects

The definition of the subjects

- Manufacturer,
- Personalisation Agent,
- Terminal
- Inspection System,
- Travel document holder
- Traveler
- Attacker

used in the following chapters is given in section 4.3.

7.1.2 Security Attributes

Security Attribute	Values	Meaning
Terminal Authentication Status	none (any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2

7.2 Security Functional Requirements from the Protection Profile

This section on security functional requirements covers SFRs taken from the underlying Protection Profile [1].

This section is divided into sub-section following the main security functionality.

7.2.1 SFR Class FAU

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 IC Identification Data in the audit records.
Application Note The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the travel document's chip (see FMT_MTD.1/INI_DIS).	

7.2.2 SFR Class FCS

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1	**Cryptographic key generation – Generation of Document Basic Access Keys by the TOE**
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	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [2], normative appendix 5.
Application Note The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [2], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [2], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.	

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2)

FCS_CKM.4	**Cryptographic key destruction – 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.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with random or constant data**[12] that meets the following: **none**[13]
Application Note The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.	

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA	**Cryptographic operation – Hash for Key Derivation**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm **SHA-1**[14] and cryptographic key sizes none that meet the following: **FIPS 180-2**[15].
Application Note This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [2].	

FCS_COP.1/ENC	**Cryptographic operation – Encryption / Decryption 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] FCS_CKM.4 Cryptographic key destruction

[12] [assignment: cryptographic key destruction method]
[13] [assignment: list of standards]
[14][selection: SHA-1 or other approved algorithms]
[15][selection: FIPS 180-2 or other approved standards]

FCS_COP.1.1/ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm TDES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [29] and [2]; normative appendix 5, A5.3
Application Note This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.	

FCS_COP.1/AUTH	**Cryptographic operation – Authentication Personalization Agent**
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/AUTH	The TSF shall perform authentication – encryption and decryption in accordance with a specified cryptographic algorithm **AES and TDES**[16] and cryptographic key sizes **112 (TDES), 128 (AES), 192 (AES), 256 (AES)**[17] bit that meet the following: **(AES) FIPS 197** [30] **and (TDES) ISO/IEC 18033-3** [31][18].
Application Note This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).	

FCS_COP.1/MAC	**Cryptographic operation – Retail 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/MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3,

[16] [selection: AES, TDES]

[17] [selection: 112, 128, 168, 192, 256]

[18] [selection: FIPS 46-3 [30], FIPS 197 [31]]

	block cipher DES, Sequence Message Counter, padding mode 2) [32].
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 the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.	

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

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** [33][19].
Application Note This SFR requires the TOE to generate random numbers used for the authentication protocol as required by FIA_UAU.4.	

7.2.3 SFR Class FIA

The following Table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [2], normative appendix 5, and [10]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	either Triple-DES with 112 bit keys or AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow

[19] [assignment: a defined quality metric]

	1. to read the Initialization Data in Phase 2 "Manufacturing", 2. to read the random identifier in Phase 3 "Personalization of the MRTD", 3. to read the random identifier in Phase 4 "Operational Use" on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application Note The IC manufacturer and the travel document manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 "Manufacturing" of the TOE. At this time the Manufacturer is the only user role available for the TOE. The travel document manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the travel document". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System. *Application Note* In the "Operational Use" phase the travel document must not allow anybody to read the ICCSN, the travel document identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the travel document's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.	

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

FIA_UAU.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 "Manufacturing", 2. to read the random identifier in Phase 3 "Personalization of the MRTD", 3. to read the random identifier in Phase 4 "Operational Use"

	on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Application Note The Basic Inspection System and the Personalization Agent authenticate themselves.	

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4	**Single-use authentication of the Terminals by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Authentication Mechanism based on **TDES and AES**[20].
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. *Application Note* The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [2]. In the first step the terminal authenticates itself to the travel document's chip and the travel document's chip authenticates to the terminal in the second step. In this second step the travel document's chip provides the terminal with a challenge-response-pair which allows a unique identification of the travel document's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.	

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide 1. Basic Access Control Authentication Mechanism,

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

	2. Symmetric Authentication Mechanism based on **AES or Triple-DES** [21] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) **the Symmetric Authentication Mechanism with the Personalization Agent Key based on AES or DES**[22] **2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys**
Application Note In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [16] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [19] FIA_UAU.5.2). *Application Note* The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.	

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2)

FIA_UAU.6	**Re-authenticating – Re-authenticating of Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism
Application Note	

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

[22] [selection: the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]]

The Basic Access Control Mechanism specified in [2] includes the 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 Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/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 BAC user. *Application Note* Note that in case the TOE should also fulfill [16] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1
FIA_AFL.1.1	The TSF shall detect when an administrator configurable positive integer within **1 - 16**[23] **consecutive** unsuccessful authentication attempts occur related to **authentication attempts using the Basic Access Control Authentication Mechanism.**
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met**[24], the TSF shall - **activate authentication delay for following consecutive unsuccessful authentication attempts, starting with a delay of 1 second and exponentially growing[25] with each following consecutive unsuccessful attempt.**
Application Note The ST writer shall perform the open operation in the elements FIA_AFL.1.1 and FIA_AFL.1.2. These assignments should be assigned to ensure especially the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential. The ST writer may consider the following example for such operations and refinement: FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 consecutive unsuccessful authentication attempts occur related to BAC authentication protocol. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time between the receiving the terminal challenge e IFD and sending the TSF response e ICC during the	

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

[24] [assignment: met or surpassed]

[25] [assignment: list of actions]

BAC authentication attempts. The terminal challenge e IFD and the TSF response e ICC are described in [34], Appendix C. The refinement by inclusion of the word “consecutive” allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the “consecutive unsuccessful authentication attempts” are count independent on power-on sessions but reset to zero after successful authentication only.

7.2.4 SFR Class FDP

The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below (Common Criteria Part 2).

FDP_ACC.1	**Subset access control – Basic Access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1
FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document.

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2).

FDP_ACF.1	**Basic Security attribute based access control – Basic Access Control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1 FMT_MSA.3 Static attribute initialisation:
FDP_ACF.1.1	The TSF shall enforce the Basic Access Control SFP to objects based on the following: 1. Subjects: a. Personalization Agent b. Basic Inspection System c. Terminal, 2. Objects: a. data EF.DG1 to EF.DG16 of the logical travel document, b. data in EF.COM, c. data in EF.SOD, 3. Security attributes: a. authentication status of terminals.

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document, 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical travel document.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical travel document. 2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical travel document. 3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4
Application Note The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this protection profile (cf. [16] for details).	

FDP_UCT.1 and FDP_UIT.1 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 authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1	**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 [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1
FDP_UCT.1.1	The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

FDP_UIT.1	**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 [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1
FDP_UIT.1.1	The TSF shall enforce the Basic 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	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

7.2.5 SFR Class FMT

The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (Common Criteria Part 2).

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

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (Common Criteria Part 2).

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

	3. Basic Inspection System.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
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.*	

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

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 disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and, 4. substantial information about construction of TSF to be gathered which may enable other attacks.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

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 disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and, 4. substantial information about construction of TSF to be gathered which may enable other attacks
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. Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software. *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.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA	**Management of TSF data – Writing of Initialization Data and Pre-personalization Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.
Application Note The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.	

FMT_MTD.1/INI_DIS	**Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.
Application Note According to P.Manufact the IC Manufacturer and the travel document Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre- personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The travel document Manufacturer will write the Pre-personalization Data.	

FMT_MTD.1/KEY_WRITE	**Management of TSF data – Key Write**
Hierarchical to:	No other components.

Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

FMT_MTD.1/KEY_READ	**Management of TSF data – Key Read**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read the Document Basic Access Keys to none.

7.2.6 SFR Class FPT

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

The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below (Common Criteria Part 2 extended).

FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit **variations in IC power consumption or electromagnetic emissions or variations in command execution time**[26] in excess of **non-useful information**[27] enabling access to Personalization Agent Key(s) **and Document Basic Access Keys and User Data**.[28].
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access

[26] [assignment: types of emissions]

[27] [assignment: specified limits]

[28] [assignment: list of types of user data]

	to Personalization Agent Key(s**) and Document Basic Access Key(s) and User Data**[29].
Application Note The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.	

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

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

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 out-of-range operating conditions where therefore a malfunction could occur, 2. failure detected by TSF according to FPT_TST.1.

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

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**

[29] [assignment: list of types of user data]

	• **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[30]** [31] 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.
Application Note The ST writer shall perform the operation in FPR_TST.1.1. If the travel document's chip uses state of the art smart card technology it will run the some self tests at the request of the authorized 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 "authorized user" Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.	

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

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. *Application Note* The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [25]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.	

[30] [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]]

7.3 Additional Security Functional Requirements (Active Authentication)

The SFRs listed in this section cover the additional security functional requirements due to the provided optional authentication mechanism Active Authentication from [2].

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**[32] in accordance with a specified cryptographic algorithm **ECDSA**[33] and cryptographic key sizes **256, 320, 384, 512,521**[34] that meet the following: BSI TR-03111 [10][35].
Application Note 1. SFR FCS_COP.1/AA_SGEN_EC is added to contents of PPs [1]. 2. The signature generation is used to perform Active Authentication.	

FCS_COP.1/AA_SGEN_RSA	**Cryptographic operation – Signature generation for AA with RSA**
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_RSA	The TSF shall perform **digital signature generation**[36] in accordance with a specified cryptographic algorithm RSA[37] and cryptographic key sizes **2048 to 4096**[38] that meet the following: **ISO/IEC 9796-2 according to paragraph B.6** [39] [35]**.**
Application Note 1. SFR FCS_COP.1/AA_SGEN_EC is added to contents of PPs [1]. 2. The signature generation is used to perform Active Authentication.	

[32] [assignment: list of standards]
[33] [assignment: cryptographic algorithm]
[34] [assignment: cryptographic key sizes]
[35] [assignment: list of standards]
[36] [assignment: list of standards]
[37] [assignment: cryptographic algorithm]
[38] [assignment: cryptographic key sizes]
[39] [assignment: list of standards]

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**[40] and specified cryptographic key sizes **256, 320, 384, 512, 521**[41] that meet the following: **ANSI X9.62-2005 and ISO/IEC 15946-1:2002**[42].
Application Note 1.FCS_CKM.1/AA_EC_KeyPair is added to contents of PP [1]. 2.With FCS_CKM.1/AA_EC_KeyPair the TOE is able to create an EC key pair for Active Authentication.	

FCS_CKM.1/AA_RSA_KeyPair	**Cryptographic key generation – RSA 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_RSA_KeyPair	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA key generation**[43] and specified cryptographic key sizes **2048 to 4096**[44] that meet the following: **ISO/IEC 9796-2 according to paragraph B.6**[45] [35].
Application Note 1.FCS_CKM.1/AA_RSA_KeyPair is added to contents of PP [1]. 2.With FCS_CKM.1/AA_RSA_KeyPair the TOE is able to create an RSA key pair for Active Authentication.	

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

[40] [assignment: cryptographic key generation algorithm]

[41][assignment: cryptographic key sizes]

[42] [selection: based on the Diffie-Hellman key derivation protocol compliant to [38] and [10], based on an ECDH protocol compliant to [37]]

[43] [assignment: cryptographic key generation algorithm]

[44][assignment: cryptographic key sizes]

[45] [assignment: list of standards]

FIA_API.1.1/AA	The TSF shall provide an **Active Authentication Protocol according to** [2][46] to prove the identity of the **TOE**[47].
Application Note This SFR requires the TOE to implement the Active Authentication Mechanism specified in [2]. The TOE computes a signature over a nonce received from the terminal, sends the signature to the terminal and the terminal verifies the signature.	

FMT_MTD.1/AA_PK	**Management of TSF data – 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/ AA_PK	The TSF shall restrict the ability to create or load[48] the **Active Authentication Private Key**[49] to Personalization Agent[50].
Application Note The verb "load" means here that the Active Authentication Private Key are generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Active Authentication Private Key is generated by the TOE itself. This TOE is able to generate the Active Authentication Private Keys, see FCS_CKM.1/AA_EC_KeyPair and FCS_CKM.1/AA_RSA_KeyPair.	

7.4 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

- ADV_FSP.5
- ADV_INT.2
- ADV_TDS.4
- ALC_CMS.5
- ALC_DVS.2
- ALC_FLR.1
- ALC_TAT.2
- ATE_DPT.3

[46] [assignment: *authentication mechanism*]
[47] [assignment: *authorized user or role*]
[48] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[49] [assignment: list of TSF data]
[50] [assignment: the authorised identified roles]

7.5 Security Requirements Rationale

7.5.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	**OT.Active_Auth_Proof**
FAU_SAS.1				x					
FCS_CKM.1	x	x	x						
FCS_CKM.4	x		x						
FCS_COP.1/SHA	x	x	x						
FCS_COP.1/ENC	x	x	x						
FCS_COP.1/AUTH	x	x							
FCS_COP.1/MAC	x	x	x						
FCS_RND.1	x	x	x						
FIA_UID.1			x	x					
FIA_AFL.1			x	x					
FIA_UAU.1			x	x					
FIA_UAU.4	x	x	x						
FIA_UAU.5	x	x	x						
FIA_UAU.6	x	x	x						
FDP_ACC.1	x	x	x						
FDP_ACF.1	x	x	x						
FDP_UCT.1	x	x	x						
FDP_UIT.1	x	x	x						
FMT_SMF.1	x	x	x						
FMT_SMR.1	x	x	x						
FMT_LIM.1								x	
FMT_LIM.2								x	
FMT_MTD.1/INI_ENA				x					
FMT_MTD.1/INI_DIS				x					
FMT_MTD.1/KEY_WRITE	x	x	x						
FMT_MTD.1/KEY_READ	x	x	x						
FPT_EMSEC.1	x				x				
FPT_TST.1					x		x		
FPT_FLS.1	x				x		x		
FPT_PHP.3	x				x	x			
FCS_COP.1/AA_SGEN_EC									x
FCS_COP.1/AA_SGEN_RSA									x
FCS_CKM.1/AA_EC_KeyPair									x
FCS_CKM.1/AA_RSA_KeyPair									x
FIA_API.1/AA									
FMT_MTD.1/AA_PK									

Coverage of Security Objective for the TOE by SFR

The security objective **OT.AC_Pers** “Access Control for Personalization of logical travel document” addresses the access control of the writing the logical travel document. The write access to the logical travel document data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: 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 only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [16] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** “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. The write access to the logical travel document data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4) . The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical travel document data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical travel document data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical travel document data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical travel document (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical travel document (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control AuthenticationMechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

The security objective **OT.Identification** “Identification and Authentication of the TOE” address the storage of the IC Identification Data uniquely identifying the travel document’s chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the travel document’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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_EMSEC.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.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.

The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity" requires the TOE to use the Active Authentication mechanism as defined in [2] which is covered by FIA_API.1/AA. The Active Authentication mechanism uses cryptographic signatures which is covered by FCS_COP.1/AA_SGEN_EC and FCS_COP.1/AA_SGEN_RSA. The generated signatures make use of key material that is covered in FCS_CKM.1/AA_EC_KeyPair and FCS_CKM.1/AA_RSA_KeyPair. The material itself can only be created or loaded by the Personalization Agent which is covered in FMT_MTD.1/AA_PK.

7.5.2 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 analyzed, and non-dissolved dependencies are appropriately explained.

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

SFR	Dependencies	Support of Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC, **FCS_COP.1/AA_SGEN_EC, FCS_COP.1/AA_SGEN_RSA** Fulfilled by FCS_CKM.4

FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1 **FCS_CKM.1/AA_EC_KeyPair** **FCS_CKM.1/AA_RSA_KeyPair**
FCS_COP.1/SHA	[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	justification 1 for non-satisfied dependencies, Fulfilled by FCS_CKM.4
FCS_COP.1/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, Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[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	justification 2 for non-satisfied dependencies justification 2 for non-satisfied dependencies
FCS_COP.1/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 key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.

FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
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/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

FCS_COP.1/AA_SGEN_EC	**FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction**	**Fulfilled by FCS_CKM.1/AA_EC_KeyPair Fulfilled by FCS_CKM.4**
FCS_COP.1/AA_SGEN_RSA	**FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction**	**Fulfilled by FCS_CKM.1/AA_RSA_KeyPair Fulfilled by FCS_CKM.4**
FCS_CKM.1/AA_EC_KeyPair	**FCS_COP.1 Cryptographic operation FCS_CKM.4 Cryptographic key destruction**	**Fulfilled by FCS_COP.1/AA_SGEN_EC Fulfilled by FCS_CKM.4**
FCS_CKM.1/AA_RSA_KeyPair	**FCS_COP.1 Cryptographic operation FCS_CKM.4 Cryptographic key destruction**	**Fulfilled by FCS_COP.1/AA_SGEN_RSA Fulfilled by FCS_CKM.4**
FIA_API.1/AA	**No dependencies**	**n.a.**
FMT_MTD.1/AA_PK	**FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles**	**Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1**

Dependencies between the SFR for the TOE

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

No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

No. 3: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization 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. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the travel document and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

7.5.3 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 ADV_FSP.5 provides a much higher assurance than the pre-defined EAL4 package due to requiring the functional specification being written in semi-formal style and providing additional error information.

The selection of the component ADV_TDS.4 provides a higher assurance than the pre-defined EAL4 package due to requiring the design specification to be written in semi-formal style and to categorize each module in regard to SFR implementation.

The selection of the component ADV_INT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the entire TSF beeing well structured.

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.3 provides a much higher assurance than the pre-defined EAL4 package due to requiring the functional testing of all modules.

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 list 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.

Dependencies Rationale

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.3 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_TDS.4 Semiformal modular design
- ADV_FUN.1 Functional testing

All of these are either met or exceeded in the EAL4 assurance package and due to the augmentation.

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.

The component ADV_FSP.5 has the following dependencies:

- ADV_TDS.1 Basic design

- ADV_IMP.1 Implementation representation of the TSF

All those are met or exceeded in the EAL4 assurance package.

The component ADV_INT.1 has the following dependencies:

- ADV_IMP.1 Implementation representation of the TSF
- ADV_TDS.1 Basic modular design
- ALC_TAT.1 Well-defined development tools

All those are met or exceeded in the EAL4 assurance package.

The component ADV_TDS.4 has the following dependency:

- ADV_FSP.5 Complete semi-formal functional specification with additional error information

which is met due to the augmentation.

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

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 for the TOE 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

This TOE provides the following Security Services:

- Identification and Authentication
- Access Control
- Cryptographic Operations
- Data 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. Basic Inspection System.

according to FMT_SMR.1.

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

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”

Proof of Authenticity of Chip

This service allows to prove the authenticity the TOE’s chip using the Active Authentication mechanism (FIA_API.1/AA) by generating ECDSA or RSA signatures (FCS_COP.1/AA_SGEN_EC, FCS_COP.1/AA_SGEN_RSA) using ECC or RSA keys (FCS_CKM.1/AA_EC_KeyPair, FCS_CKM.1/AA_RSA_KeyPair) that have been created or loaded by the Personalization Agent (FMT_MTD.1/AA_PK).

Passive Authentication

This service provides the Passive Authentication according to [2].

Basic Access Control Authentication Mechanism

This service provides the BAC according to [2] (FIA_UAU.5) using Document Basic Access Key Derivation Algorithm (FCS_CKM.1, FCS_RND.1) to establish secure messaging (FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FIA_UAU.6, FDP_UIT.1, FDP_UCT.1) between the Terminal and the travel document. After the secure messaging session, the keys and authentication data are securely destroyed (FCS_CKM.4, FIA_UAU.4).

The TOE verifies that each command was sent by the Inspection System that was successfully authenticated using the BAC Authentication Mechanism by verifying the MAC (FIA_UAU.6).

After three consecutive authentication attempts have been detected an exponentially growing delay is introduced (FIA_AFL.1).

Symmetric Authentication Mechanism for Personalization Agents
This service provides the Authentication Mechanism based on TDES and AES according to [2] (FIA_UAU.5, FCS_COP.1/AUTH).

Symmetric Authentication Mechanism securely destroys keys and authentication data (FCS_CKM.4, FIA_UAU.4) after usage.

8.1.2 Access Control

This service provides access control to protect data from unauthorized disclosure.

Read Access
Only a successfully authenticated Basic Inspection System is allowed to read data on the TOE (FDP_ACF.1.2).

Access Keys on the TOE cannot be read by any entity (FMT_MTD.1/KEY_READ).

Only the Personalization Agent can disable read access to the Initialization Data (FMT_MTD.1/INI_DIS.)

Write Access
The manufacturer in the role of the IC manufacturer writes the Initialisation Data (FMT_SMF.1) 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 (FMT_SMF.1) 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).

At life-cycle Personalization only terminals that can be successfully authenticated as Personalization Agent are authorized to read and write data (FMT_SMF.1, FMT_MTD.1/KEY_WRITE) on the TOE (FDP_ACF.1.2).

8.1.3 Cryptographic Operations

This service provides a true random number generator (FCS_RND.1) to allow secure authentication using the Basic Access Control Authentication Mechanism and the Symmetric Authentication Mechanism based on TDES and AES.

This service provides signature generation (FCS_COP.1/AA_SGEN_EC, FCS_COP.1/AA_SGEN_RSA) to allow proof of chip's authenticity using Active Authentication Mechanism (FIA_API.1/AA).

This service is able to generate keys (FCS_CKM.1, FCS_CKM.1/AA_EC_KeyPair FCS_CKM.1/AA_RSA_KeyPair) that are used for authentication and secure messaging purposes.

8.1.4 Data Confidentiality

This service provides the secure messaging in MAC-ENC mode (FCS_COP.1/MAC, FCS_COP.1/ENC).

Secure Messaging
After successfully running the BAC Authentication Mechanism this service provides a TDES encrypted (FCS_COP.1/ENC) data stream between an authenticated entity and the TOE.

8.1.5 Data Integrity

Secure Messaging

This service provides protection from modification, deletion, insertion and replay of transmitted data (FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FIA_UAU.6, FDP_UIT.1, FDP_UCT.1).

This service provides the Secure messaging in MAC-ENC mode (FCS_COP.1/MAC, FCS_COP.1/ENC).

After successfully running the BAC Authentication Mechanism this service provides an integrity protected (FCS_COP.1/MAC) data stream using Retail-MAC between an authenticated entity and the TOE. The BAC Authentication Mechanism uses sessions keys agreed upon according to [2] (FCS_CKM.1).

In case an error occurs during secure messaging communication, i.e. a command cannot be verified (FCS_COP.1/MAC, FIA_UAU.6) the session keys are destroyed (FCS_CKM.4).

Integrity Self Test

This service runs file system integrity self-test after reset on OS start-up (FPT_TST.1).

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 run on the TOE which integrity is verified. (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 or information (code, chip layout) about the TOE to be leaked to allow an attacker 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) 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 (FPT_EMSEC.1).

Software (IC embedded software)

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

If the TOE detects a configurable number of consecutive unsuccessful authentication/verification attempts using the Basic Access Control Authentication Mechanism a delay of 1 second will be in place for following authentication attempts (FIA_AFL.1). 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 allows only the Personalisation Agent to write the Document Basic Access Keys (FMT_MTD.1/KEY_WRITE).

This service allows the Personalisation Agent in life-cycle phase 3 to create or load the Active Authentication Private Key (FMT_MTD.1/AA_PK).

8.2 Statement of Compatibility

This section shows the compatibility of this Composite ST and the Platform-ST as required by [36].

The Platform-ST is the security target of Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 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 ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2, ATE_DPT.3, ALC_FLR.1, ALC_CMS.5, ALC_TAT.2.

Therefore the Composite's Security Assurance Requirements is a subset of the Platform's Security Assurance Requirements.

8.2.2 Assumptions

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 operational environment inherited from [14]	Meaning	Operational Environment of this TOE
A.Resp-Appl	Treatment of User Data	OT.Data_Int OT.Data_Conf 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	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Inf_Leak	OT.Prot_Abuse-Func	OT.Identification	OT.Active_Auth_Proof	OT.Data_Int	OT.Data_Conf
O.Phys-Manipulation	x						x	
O.Phys-Probing	x		x			x		x
O.Malfunction	x	x						
O.Leak-Inherent			x			x		x
O.Leak-Forced			x			x		x
O.Abuse-Func			x	x				x
O.Identification					x			
O.RND	x					x		
O.Cap_Avail_Loader				x				
O.Ctrl_Auth_Loader				x				
O.AES							x	x
O.TDES							x	x
O.RSA						x		
O.ECC						x		
O.AES-CMAC							x	x
O.TDES-RMAC							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 can not be mapped to OTs of this ST

- O.Firewall
- O. Authentication
- O.FFC
- O.Hash

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.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 tis 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.Resp-Appl
- OE.Process-Sec-IC
- OE.Lim_Block_Loader
- OE.Loader_Usage
- OE.TOE_Auth

According to the Note after Table 13, Page 18 of the Security Target the objective OE.TOE_Auth only applies when the Flash Loader is available.

This is only 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.

The same applies for OE.Loader_Usage, therefore OE.Lim_Block_Loader and OE.Loader_Usage are rated as Ir.OE[51] as they address the TOE Manufacturer in the sense of the Chip Hardware Certification.

The objective OE.Resp-Appl covers the protection especially confidentiality of the user data which are completely protected by the TOE core functionality itself and is therefore rated as CfPOE.

The following tables gives a summary for the rating and mapping of the platform OEs to TOE SFRs where applicable.

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

Objective for the Operational Environment in the HW platform ST	Meaning	Classification	Operational Environment / SFRs of this TOE
OE.Resp-Appl	Treatment of user data of the Composite TOE	CfPOE	FCS_CKM.4, FIA_AFL.1, FIA_UID.1, FIA_UAU, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_LIM.1 FMT_LIM.2, FMT_MTD.1, FPT_FLS.1, FPT_TST.1, FPT_PHP3, FPT_EMSEC.1
OE.Process-Sec-IC	Protection during composite product manufacturing	Ir.OE	n/a
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	Ir.OE	n/a
OE.Loader_Usage	Secure communication and usage of the Loader	Ir.OE	n/a

[51] In the sense of ASE_COMP.1

OE.TOE_Auth	External entities authenticating of the TOE	Ir.OE	n/a

8.2.5 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[52]	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_EMSEC.1
FDP_IFC.1	Subset Information Flow Control	RP_SFR-MECH	FPT_EMSEC.1
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	RP_SFR-MECH	FPT_EMSEC.1
FCS_RNG.1/CS/PTG3	Cryptographic Operation	RP-SFR-SERV	FCS_CKM.1/AA_RSA_KeyPair, (RSA Key Pair generation for AA) FCS_CKM.1/AA_EC_KeyPair (EC Key Pair generation for AA) FCS_RND.1
FCS_RNG.1/TRNG	Cryptographic Operation	RP-SFR-SERV	FPT_EMSEC.1 (blinding/masking)
FPT_TST.1	TSF Testing	RP_SFR-MECH	FPT_TST.1 FPT_PHP.3
FCS_CKM.1/CS/EC	Cryptographic operation	RP-SFR-SERV	FCS_CKM.1/AA_EC_KeyPair,
FCS_CKM.1/CS/RSA	Cryptographic operation	RP-SFR-SERV	FCS_CKM.1/AA_RSA_KeyPair,
FCS_COP.1/CS/ECC	Cryptographic Operation	RP-SFR-SERV	FCS_COP.1/AA_SGEN_EC
FCS_COP.1/CS/RSA	Cryptographic Operation	RP-SFR-SERV	FCS_COP.1/AA_SGEN_RSA
FCS_CKM.4/CS/ECC	Cryptographic key destruction	RP-SFR-SERV	FCS_CKM.4

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

FCS_CKM.4/CS/RSA	Cryptographic key destruction		FCS_CKM.4
FCS_COP.1/TDES	Cryptographic operation	RP-SFR-SERV	FCS_COP.1/ENC, FCS_COP.1/MAC FCS_COP.1/AUTH
FCS_COP.1/AES	Cryptographic Support (AES)	RP-SFR-SERV	FCS_COP.1/AUTH
FCS_CKM.4/AES	Cryptographic key destruction	RP_SFR-MECH	FCS_CKM.4
FCS_CKM.4/TDES	Cryptographic key destruction	RP_SFR-MECH	FCS_CKM.4
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.2	Complete Access Control	RP_SFR-MECH	FPT_FLS.1
FDP_ACF.1	Security Attribute Based Access Control	RP_SFR-MECH	FPT_FLS.1
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_EMSEC.1, FPT_FLS.1, FPT_PHP.3
FMT_MSA.3	Static Attribute Initialization	RP_SFR-MECH	FPT_EMSEC.1, FPT_FLS.1, FPT_PHP.3
FMT_SMF.1	Specification of Management Functions	RP_SFR-MECH	FPT_FLS.1, FPT_PHP.3
FMT_SMR.1	Security Roles	RP_SFR-MECH	FPT_FLS.1, FPT_PHP

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
Active Authentication	Security mechanism defined in [2] 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 [2] 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 (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 [2].
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.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means [2].
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
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K ENC) and message authentication (key K MAC) of data transmitted between the travel document's chip and the inspection system [2]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
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) [2].
Eavesdropper	A threat agent with basic enhanced 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 [2].

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	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 [2], 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.
Extended Access Control	Security mechanism identified in [2] 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 [2].
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to 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. [2]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different 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. [2]

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. [2]
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. [2]
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). [2]
Issuing State	The Country issuing the travel document. [2]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [2]. 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 [2] 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. [2]
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. [2] 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. [2]
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
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 [2] (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. [2]
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. [2]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to [4], [20], [2].
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 [2] (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, [2], 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. [2]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

10 Bibliography

[1] *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.*

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

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

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

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

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

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

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

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

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

[11] *EN 419212 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1 to Part 5.*

[12] *Common Criteria Public Security Target, Infineon Security Controller, IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 with optional crypro Suite.*

[13] "Certification Report BSI-DSZ-CC-1229-V2-2024".

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

[15] Security Target - ACOS-IDv4.1 eMRTD (A) EAC/PACE configuration, public version.

[16] *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..*

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

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

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

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

[21] *Preparation and Operational Manual - ACOS-IDv4.1 eMRTD, BAC and PACE/EAC configuration, Version 3.45, Date 2024-09-24.*

[22] *User Manual, Version 4.05, Date 20.09.2024.*

[23] *Internal Operation Manual, Version 2.1, 2024-04-11.*

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

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

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

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

[28] *PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001.*

[29] *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology.*

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

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

[32] *ISO/IEC 9797-1:2011, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011.*

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

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

[35] *ISO/IEC 9796-2:2010 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms, Edition 3, 2010.*

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

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

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