



TMCICAO v1.0 on TMCOS 4.0 0.5
in ICAO EAC with PACE configuration
Security Target Lite
Common Criteria EAL5+

Revision History

Rev	Date	Description
1.0	2026-4-9	ST Lite Public Release
1.1	2026-4-17	Chapter 1.1: Update version and publication date Chapter 8: Modify the reference
1.2	2026-4-23	Chapter 1.1: Update version and publication date Chapter 8: Modify the reference

Content

Content	- 3 -
List of figures	- 5 -
List of tables	- 6 -
1 ST Introduction.....	- 7 -
1.1 ST Reference	- 7 -
1.2 TOE Reference	- 7 -
1.3 TOE Overview	- 7 -
1.3.1 TOE Type	- 7 -
1.3.2 TOE Usage & Major Security Features	- 7 -
1.3.3 Required Non-TOE Hardware/Software/Firmware	- 10 -
1.4 TOE Description.....	- 10 -
1.4.1 TOE Physical Scope	- 10 -
1.4.2 TOE Logical Scope	- 11 -
1.4.3 TOE Life Cycle	- 13 -
2 Conformance Claims	- 17 -
2.1 CC Conformance Claim	- 17 -
2.2 CC PP Claim.....	- 17 -
2.3 CC Package Claim.....	- 17 -
2.4 Conformance Rationale	- 17 -
2.4.1 Conformity of the TOE type.....	- 18 -
2.4.2 SPD Consistency	- 18 -
2.4.3 Security Objectives Consistency	- 21 -
2.4.4 Conformity of the Requirement (SFR/SAR)	- 22 -
3 Security Problem Definition.....	- 25 -
3.1 Introduction	- 25 -
3.2 Assumptions	- 25 -
3.3 Threats.....	- 25 -
3.4 Organizational Security Policies	- 25 -
4 Security Objectives	- 26 -
4.1 Security Objectives for the TOE	- 26 -
4.2 Security Objectives for the Operational Environment.....	- 26 -
4.3 Security Objectives Rationale	- 26 -
4.3.1 Rationale between Objectives and SPD	- 26 -
4.3.2 Compatibility between Objectives of the TOE and [TMC_IC].....	- 28 -
5 Extended Components Definition	- 30 -
5.1 Definition of the Family FAU_SAS	- 30 -
5.1.1 Family behavior.....	- 30 -
5.1.2 Component leveling and description	- 30 -
5.1.3 Management of FAU_SAS.1	- 30 -
5.1.4 Audit of FAU_SAS.1.....	- 30 -
5.1.5 FAU_SAS.1 Audit storage.....	- 30 -
6 Security Requirements	- 31 -

6.1	Security Functional Requirements	- 35 -
6.1.1	Class FCS Cryptographic Support.....	- 35 -
6.1.2	Class FIA Identification and Authentication.....	- 42 -
6.1.3	Class FDP User Data Protection.....	- 46 -
6.1.4	Class FMT Security Management	- 48 -
6.1.5	Class FPT Protection of the Security Functions	- 49 -
6.2	Security Assurance Requirements	- 51 -
6.3	Security Requirements Rationale	- 51 -
6.3.1	Dependency Rationale.....	- 51 -
6.3.2	Security Functional Requirements Rationale	- 58 -
6.3.3	Security Assurance Requirements Rationale.....	- 64 -
6.3.4	Security Requirements – Mutual Support and Internal Consistency.....	- 64 -
6.3.5	Compatibility between SFRs of the TOE and [TMC_IC]	- 64 -
7	TOE Summary Specification.....	- 67 -
7.1	TSFs provided by the TMCICAO Application.....	- 67 -
7.2	TSFs provided by the IC	- 71 -
8	Appendix	- 72 -
8.1	Glossary and Acronyms.....	- 72 -
8.2	Literature	- 81 -

List of figures

Figure 1 Physical scope diagram.....	- 11 -
Figure 2 TOE Life Cycle diagram.....	- 13 -
Figure 3 FAU_SAS: Component leveling.....	- 30 -

List of tables

Table 1 Comprise of TOE	- 11 -
Table 2 Role of the TOE components in the logical scope	- 12 -
Table 3 Overview of the life cycle of Composite product	- 14 -
Table 4 TOE Deliverables	- 15 -
Table 5 Assets Consistency table	- 19 -
Table 6 Subjects Consistency table	- 20 -
Table 7 Assumptions Consistency table	- 20 -
Table 8 Threats Consistency table	- 20 -
Table 9 Organizational Security Policies Consistency table	- 21 -
Table 10 Security objectives for the TOE Consistency table	- 21 -
Table 11 Security objectives for the OE Consistency table	- 22 -
Table 12 SFR Consistency table	- 23 -
Table 13 Security Objective Rationale	- 27 -
Table 14 Objectives for the TOE and [TMC_IC] compatibility table	- 28 -
Table 15 Objectives for OE compatibility table	- 29 -
Table 16 Definition of security attributes	- 32 -
Table 17 Overview of the keys and certificates	- 34 -
Table 18 SFR list	- 35 -
Table 19 FCS_CKM.1/CA Key pair explanation	- 35 -
Table 20 FCS_CKM.1/AA explanation	- 36 -
Table 21 FCS_CKM.1/DH_PACE explanation	- 36 -
Table 22 FCS_CKM.1/CA explanation	- 37 -
Table 23 FCS_CKM.6.1 explanation	- 38 -
Table 24 FCS_CKM.6.2 explanation	- 39 -
Table 25 FCS_COP.1/PACE_ENC explanation	- 39 -
Table 26 FCS_COP.1/PACE_MAC explanation	- 40 -
Table 27 FCS_COP.1/CA_ENC explanation	- 40 -
Table 28 FCS_COP.1/SIG_VER explanation	- 40 -
Table 29 FCS_COP.1/CA_MAC explanation	- 41 -
Table 30 FCS_COP.1/AA explanation	- 41 -
Table 31 Overview on authentication SFR	- 42 -
Table 32 FIA_AFL.1.1/PACE explanation	- 43 -
Table 33 FIA_AFL.1.2/PACE explanation	- 43 -
Table 34 FPT_EMS.1.1 table	- 50 -
Table 35 SFR Dependencies	- 56 -
Table 36 Non-satisfied Dependencies	- 57 -
Table 37 SAR Dependencies	- 58 -
Table 38 Security Objective Rationale	- 59 -
Table 39 Compatibility between SFRs and [TMC_IC]	- 66 -
Table 40 Security Functions provided by the TMCICAO Application	- 68 -
Table 41 Security Functions provided by the IC	- 71 -

1 ST Introduction

1.1 ST Reference

Title:	TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE configuration Security Target Lite
Version:	V1.2
Author:	Tongxin Microelectronics Co., Ltd
Publication Date:	2026-4-23

1.2 TOE Reference

Product Type:	Contactless integrated circuit chip of machine-readable travel documents
TOE Name:	TMCICAO v1.0 on TMCOS 4.0 0.5 in EAC with PACE configuration
TOE Version:	1.0
Developer:	Tongxin Microelectronics Co., Ltd

1.3 TOE Overview

This document contains the Security Target for the TMCICAO v1.0 on TMCOS 4.0 0.5, an MRTD chip programmed according to the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods defined in the specification for Password Authenticated Connection Establishment, Extended Access Control and Active Authentication according to [ICAO9303].

1.3.1 TOE Type

The Target of Evaluation (TOE) is an electronic travel document representing a dual interface smart card programmed according to the Logical Data Structure (LDS) and providing Password Authenticated Connection Establishment, Extended Access Control and Active Authentication according to [ICAO9303], [SAC] and [TR03110-1]. The ICAO application is programmed on top of a JavaCard Platform without post-issuance loading application capacity.

1.3.2 TOE Usage & Major Security Features

TOE Usage:

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 Security Target contains

- 1) visual (eye readable) biographical data and portrait of the holder,
- 2) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine-readable zone (MRZ) and

- 3) data elements on the travel document's chip according to LDS in case of contactless machine reading.

The authentication of the traveler is based on

- 1) the possession of a valid travel document personalized for a holder with the claimed identity as given on the biographical data page and
- 2) biometrics using the reference data stored in the travel document.

The issuing State or Organization ensures the authenticity of the data of genuine travel documents. 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 part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder:

- 1) the biographical data on the biographical data page of the travel document surface,
- 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 as defined in [ICAO9303] as specified by ICAO on the dual interface integrated circuit. It presents dual interface 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 biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
- 4) the other data according to LDS (EF.DG5 to EF.DG16) and
- 5) the Document Security Object (SOD).

Major Security Feature:

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO9303]. These security measures can include the binding of the travel document's chip to the travel document.

The logical travel document is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or 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 sensitive biometrics as optional security measure in the [ICAO9303], and Password Authenticated Connection Establishment. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This Security Target addresses the protection of the logical travel document

- 1) in integrity by write-only-once access control and by physical means,
- 2) in confidentiality by the Extended Access Control Mechanism,
- 3) in confidentiality by Password Authenticated Connection Establishment (PACE) and
- 4) Active Authentication is used to prove the authenticity of the chip.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE.

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

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

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [TR03110-1], [ICAO9303].

The Security Target requires the TOE to implement the Extended Access Control as defined in [TR03110-1]. The Extended Access Control consists of two parts:

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

The Chip Authentication Protocol v.1

- 1) authenticates the travel document's chip to the inspection system and
- 2) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality

and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

Therefore, Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of

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

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

Active Authentication authenticates the chip by signing a challenge sent by the IFD (inspection system) with a private key known only to the chip. For this purpose, the chip contains its own Active Authentication Key pair. A hash representation of Data Group 15 (Public Key info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is stored in the contactless IC's secure memory.

By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair, the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD.

Additionally, the TOE supports the security features of Basic Access Control (BAC). However, this feature is outside of the scope of this Security Target.

1.3.3 Required Non-TOE Hardware/Software/Firmware

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 and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.4 TOE Description

1.4.1 TOE Physical Scope

The TOE physical scope is as follows:

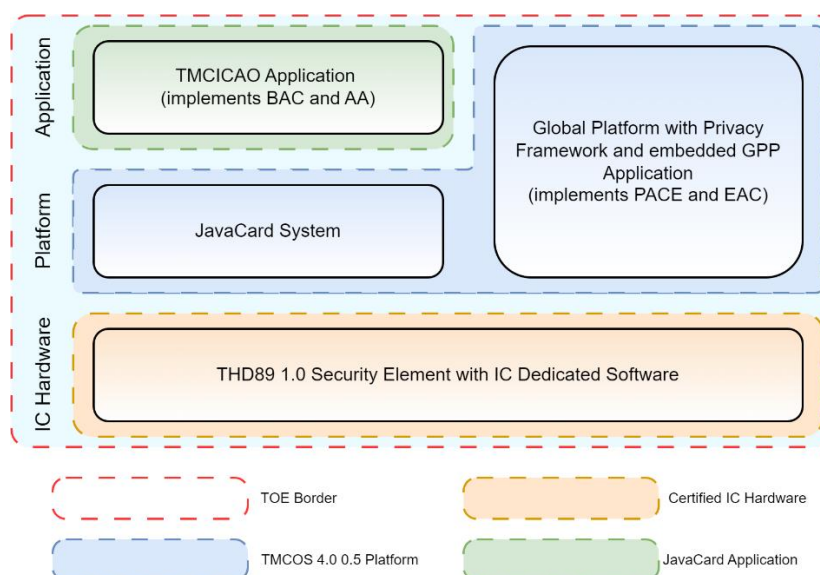


Figure 1 Physical scope diagram

This Security Target addresses the TOE in EAC with PACE configuration. The TOE consists of:

Category	Component	Version	Delivery form
HW	THD89 1.0	1.0	Courier
FW	Crypto Library	1.01	Masked in ROM
FW	CryptoECCSec library	1.20	Binary in memory
FW	tmcRSA_ECC_DH_SHA_SecurityLib Library	5.09	Binary in memory
FW	Boot code	1.0	Masked in ROM
SW	TMCICAO Application	1.0	Binary in memory
SW	TMCOS	4.0 0.5	Binary in memory
DOC	[AGD_OPE]	[AGD_OPE]	Pdf file
DOC	[AGD_PRE]	[AGD_PRE]	Pdf file
DOC	[AGD_PG]	[AGD_PG]	Pdf file
DOC	[AGD_PPG]	[AGD_PPG]	Pdf file
Key	Root keys-IMK	1.0	Pdf file
Key	Root keys-TEK	1.0	Courier

Table 1 Comprise of TOE

1.4.2 TOE Logical Scope

The role of the TOE components in the logical scope is in the following table.

Component	Description
TMCICAO Application	The eMRTD application and the implementation of BAC and AA protocols as defined in [ICAO9303].

GPP Application	GPP Application provides Privacy Protocol services and Global Master File service through GP Privacy Framework as defined in [GPPF].
JavaCard System	Includes the JC API, JCRE and JCVM functionalities.
GlobalPlatform with Privacy Framework	Includes the Dispatcher, GP API, security domain and privacy framework functionalities. It implements the EAC and PACE protocols as defined in [ICAO9303].
THD89 Security Element with IC Dedicated Software	The THD89 1.0 Security Element with IC Dedicated Software that has already been certified. It provides the following hardware security functionalities: ● Protection against malfunctions ● Leakage resistance ● Physical manipulation and probing protection ● Abuse of functionality prevention ● Unique identification ● Secure random number generation ● Robust cryptographic functionality The logical scope of hardware is described in the [TMC_IC] section 1.3.2.

Table 2 Role of the TOE components in the logical scope

The TOE is comprised of several security features. Each of the security features identified in section 1.3.2 consists of several security functionalities, as detailed below:

(1) Confidentiality protection by the Extended Access Control Mechanism:

- Chip Authentication protocol as defined in [ICAO9303]
- Terminal Authentication protocol as defined in [ICAO9303]
- CA Secure messaging

(2) Confidentiality protection by the Password Authenticated Connection Establishment (PACE):

- Asymmetric cryptography-based PACE protocol as defined in [ICAO9303]
- PACE Secure messaging

(3) Active Authentication is used to prove the authenticity of the chip:

- Active Authentication protocol as defined in [ICAO9303]

(4) Integrity protection by write-only-once access control and by physical means:

- Access control policy of the sensitive data stored on logical MRTD using SCP03
- IC-provided security features as defined in the table 2 above

1.4.3 TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP0084], the TOE life-cycle is additionally subdivided into 7 steps.)

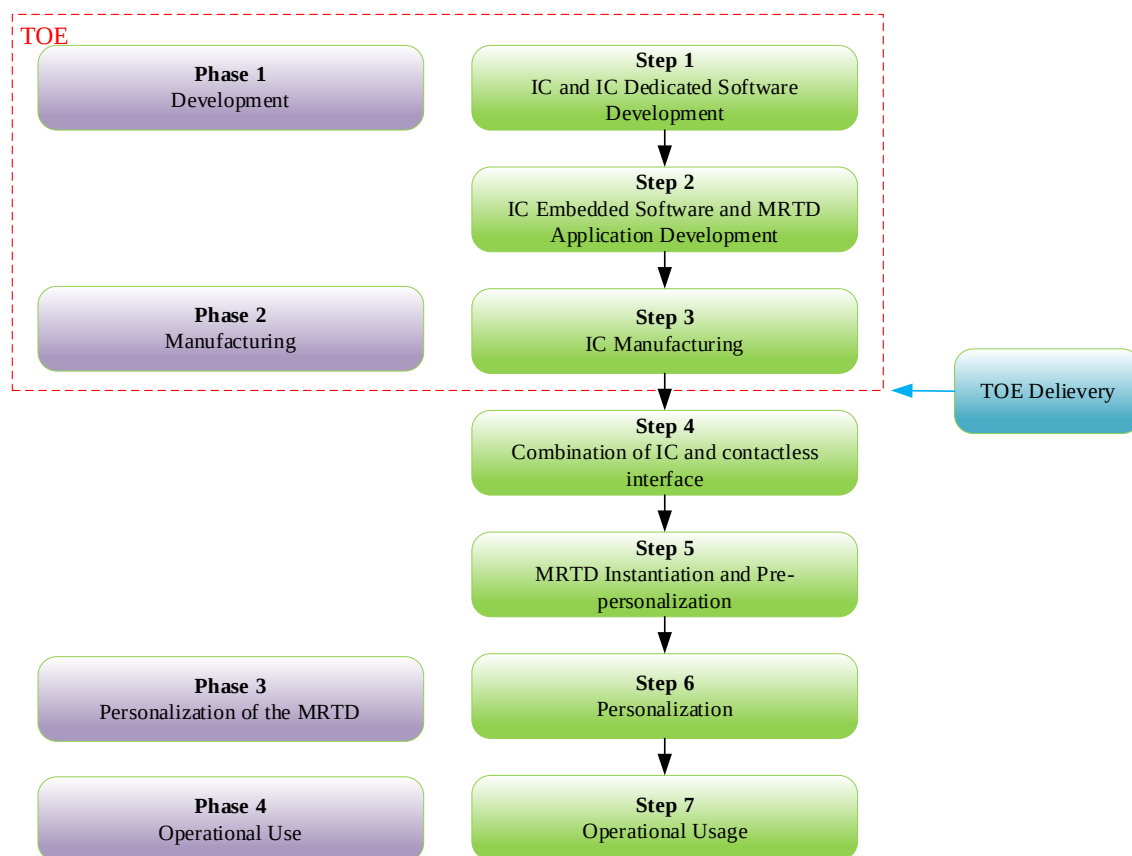


Figure 2 TOE Life Cycle diagram

The following table illustrates that the lifecycle of the Composite Product covers different steps in different sites.

Phase	Step	Site	Activity
1	1	Beijing Tongxin Microelectronics Co., Ltd.	IC design and IC dedicated software development
	2	Beijing Tongxin Microelectronics Co., Ltd.	JC System and MRTD application development
2	3a	Wafer Manufacturer	Wafer manufacturing
	3b	Wafer Manufacturer	JCS and ICAO package loading
	3c	IC Packaging Site	IC packaging
	4	Third-party MRTD Manufacturer	Combination of IC and passport book

	5	Third-party MRTD Manufacturer	Pre-Personalization
3	6	Third-party Personalization Agent	Personalization
4	7	Passport holder	Operational use

Table 3 Overview of the life cycle of Composite product

Phase 1 “Development”

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

(Step2) The TMC (SW) uses the guidance documentation for the integrated circuit, the IC Dedicated Software (Cryptographic libraries) and the relevant guidance documentation to develop the IC Embedded Software (JavaCard System, GPP Application and GlobalPlatform with Privacy Framework), the MRTD application and the guidance documentation associated with these TOE components.

The IC Dedicated Software in the non-volatile non-programmable memories (ROM), the IC Embedded Software in the non-volatile programmable memories (NVM), the ICAO package and related supporting documents are securely delivered to the IC manufacturer.

Phase 2 “Manufacturing”

(Step3a) In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated 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 MRTD material during the IC manufacturing.

(Step3b) The IC manufacturer adds the IC Embedded Software and ICAO package (TMCICAO Application) in the non-volatile programmable memories (NVM). The IC is securely delivered from IC manufacturer to the IC packaging site.

Note: the GPP Application is integrated in the IC Embedded Software.

(Step3c) The IC packaging site packages the IC.

The TOE delivery takes place at **Step3c**, thus **Step1** to **Step3c** are considered as part of the evaluation scope.

Deliverables delivered from TMC to MRTD Manufacturer are listed in the table below:

Type	Name	Version	Delivery method
Composite Product	TMCICAO v1.0 on TMCOS 4.0 0.5	1.0	Courier deliver
Document	[AGD_OPE]	[AGD_OPE]	Encrypted e-mail
	[AGD_PRE]	[AGD_PRE]	Encrypted e-mail
	[AGD_PG]	[AGD_PG]	Encrypted e-mail

	[AGD_PPG]	[AGD_PPG]	Encrypted e-mail
Key	Root keys-IMK	1.0	Encrypted e-mail
	Root keys-TEK	1.0	Courier deliver

Table 4 TOE Deliverables

The Root keys-TEK is used to protect the Root keys-IMK, the Root keys-IMK is used for the authentication of the MRTD Manufacturer.

(Step4) The travel document manufacturer combines the IC with hardware for the contactless interface in the travel document unless the travel document consists of the card only.

(Step5) The travel document manufacturer:

- 1) creates the ePassport application (i.e. the Applet instantiation), and
- 2) equips travel document's chips with pre-personalization Data.

The pre-personalized travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalization Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation ([AGD_OPE] and [AGD_PG]) and Personalization Agent Key to the Personalization Agent.

Phase 3 “Personalization of the travel document”

(Step6) The personalization of the travel document includes:

- 1) the survey of the travel document holder's biographical data,
- 2) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- 3) the personalization of the visual readable data onto the physical part of the travel document,
- 4) the writing of the TOE User Data and TSF Data into the logical travel document and
- 5) configuration of the TSF if necessary.

The step (5) is performed by the Personalization Agent and includes but is not limited to the creation of

- 1) the digital MRZ data (EF.DG1),
- 2) the digitized portrait (EF.DG2), and
- 3) the Document security object.

The signing of the Document security object by the Document signer [ICAO9303] finalizes the personalization of the genuine travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

Phase 4 “Operational Use”

(Step7) The TOE is used as a travel document's chip by the traveler 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

Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note: The authorized Personalization Agents is not allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This implies that an update of the Document Security Object including the re-signing by the Document Signer is not allowed.

Note, that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under [AGD_OPE] and [AGD_PRE].

2 Conformance Claims

2.1 CC Conformance Claim

The Security Target claims conformance to

- CC Part 1 conformant [CC:2022 P1],
- CC Part 2 extended [CC:2022 P2],
- CC Part 3 conformant [CC:2022 P3] and
- CC Part 5 conformant [CC:2022 P5].

The following methodology is used for the TOE evaluation:

- CC Evaluation methodology [CEM:2022].

The following documentations are used as the supporting references in this Security Target:

- Transition Policy to CC:2022 and CEM:2022: [CC:TP] and
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1): [CC:EI].

2.2 CC PP Claim

The Security Target claims strict conformance to [PP0056], and [PP0056] claims strict conformance to [PP0068].

2.3 CC Package Claim

The Security Target claims conformance to the assurance package EAL5 augmented with:

- ALC_DVS.2,
- ALC_FLR.1 and
- AVA_VAN.5

defined in CC Part 5 [CC:2022 P5].

The Security Target claims conformance to the composite product package COMP defined in CC Part 5 [CC:2022 P5].

2.4 Conformance Rationale

Conformance rationale of the ST against [PP0056] and [PP0068] is mapped below. The conformance rationale focuses on assets, threats, OSPs, assumptions, security objectives, and SFRs and the notation used is detailed below:

- Equivalent (E): The element in the ST is the same as in [PP0056] or [PP0068].
- Refinement (R): The element in the ST refines the corresponding [PP0056] or [PP0068] element. New names are given between brackets and added to the list of elements.
- Addition (A): The element is newly defined in the ST; it is not present in [PP0056] or [PP0068] and does not affect it.
- Modification (M): The element in the ST is adapted according the [CC:2022 P2].
- X: The element is present in [PP0056] or [PP0068], if the element presented in both [PP0056] and [PP0068], then the definition of the element follows the description in [PP0056].

This ST adopts the new version of ICAO Doc9303 Eighth Edition [ICAO9303] as reference. Due to this update, any references to the ICAO Doc9303 Sixth Edition in the PP have been replaced with references to ICAO Doc9303 Eighth Edition in this ST.

This ST also adopts the new version of BSI TR-03110 series technical guidelines as reference. This new version includes the specification of the EAC mechanism. Due to this update, any reference to the former versions of BSI TR-03110 in the PPs have been replaced with references to TR-03110-1 Version 2.20 in this ST.

The content of some “Application notes” present in [PP0056] and [PP0068] may have been omitted or modified in this ST to avoid possible conflicts and inconsistencies of references / terminology / requirements used in these PPs claiming conformance to CC v3.1 while this ST claims conformance to CC:2022. Since the “Application note” is an 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, a reader of this ST may refer to the respective “Application notes” from [PP0056] and [PP0068]. The applicable “Application notes” shall be read and interpreted in the context of CC:2022.

2.4.1 Conformity of the TOE type

The TOE is an electronic travel document representing a dual interface (contact and contactless) smart card programmed according to the Logical Data Structure (LDS) and providing Password Authenticated Connection Establishment, Extended Access Control and Active Authentication according to [ICAO9303]. This is consistent with the TOE type defined in the PPs [PP0056] and [PP0068].

In addition to the contactless interface referred in the [PP0056] and [PP0068], this ST makes also references to the contact interface according to [ISO7816-2] since the TOE supports both interfaces. The use of the final TOE (after delivery from the Personalization Agent to the MRTD Holder) coincides with the intended use according to [PP0056] and [PP0068].

In addition to Extended Access Control and Password Authenticated Connection Establishment, the TOE also implements Active Authentication. This is consistent with the TOE type in the [PP0056] and [PP0068], as Active Authentication does not contradict or compromise the functionality provided by either of these mechanisms. Specifically, Active Authentication provides an alternative mechanism to Chip Authentication for the authentication of the eMRTD.

2.4.2 SPD Consistency

2.4.2.1 Assets consistency

All assets defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the assets' consistency.

Assets	PP0068	PP0056	Security Target
User data stored on the TOE	X		(E)
User data transferred between the TOE and the terminal	X		(E)
Travel document tracing data	X		(E)
Accessibility to the TOE functions and data only for authorized subjects	X		(E)
Genuineness of the TOE	X		(E)
TOE internal secret cryptographic keys	X		(E)
TOE internal non-secret cryptographic material	X		(E)
travel document communication establishment authorization data	X		(E)
Logical travel document sensitive user data		X	(E)
Authenticity of the travel documents' chip		X	(E)

Table 5 Assets Consistency table

2.4.2.2 Subjects consistency

All Subjects and external entities defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the Subjects' consistency.

Subjects	PP0068	PP0056	Security Target
Travel document holder	X		(E)
Travel document presenter (traveler)	X		(E)
Terminal	X	X	(E)
Basic Inspection System with PACE (BIS-PACE)	X		(E)
Document Signer (DS)	X		(E)
Country Signing Certification Authority (CSCA)	X		(E)
Personalization Agent	X		(E)
Manufacturer	X		(E)
Attacker	X	X	(E)
Country Verifying Certification Authority (CVCA)		X	(E)
Document Verifier (DV)		X	(E)
Inspection system (IS)		X	(E)

Extended Inspection System (EIS)		X	(E)
----------------------------------	--	---	-----

Table 6 Subjects Consistency table

2.4.2.3 Assumptions consistency

All Assumptions defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the Assumptions' consistency.

Assumptions	PP0068	PP0056	Security Target
A.Passive_Auth	X		(E)
A.Insp_Sys		X	(E)
A.Auth_PKI		X	(E)

Table 7 Assumptions Consistency table

2.4.2.4 Threats consistency

All Threats defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the Threats' consistency.

Threats	PP0068	PP0056	Security Target
T.Skimming	X		(E)
T.Eavesdropping	X		(E)
T.Tracing	X		(E)
T.Forgery	X		(E)
T.Abuse-Func	X		(E)
T.Information_Leakage	X		(E)
T.Phys-Tamper	X		(E)
T.Malfunction	X		(E)
T.Read_Sensitive_Data		X	(E)
T.Counterfeit		X	(E)

Table 8 Threats Consistency table

2.4.2.5 Organizational Security Policies consistency

All Threats defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the OSPs' consistency.

OSP	PP0068	PP0056	Security Target
P.Manufact	X		(E)
P.Pre-Operational	X		(E)
P.Card_PKI	X		(E)
P.Trustworthy_PKI	X		(E)

P.Terminal	X		(E)
P.Sensitive_Data		X	(E)
P.Personalization		X	(E)

Table 9 Organizational Security Policies Consistency table

2.4.3 Security Objectives Consistency

2.4.3.1 Objective for the TOE consistency

All Security Objectives for the TOE defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the Security Objectives' consistency and the additions.

O.TOE	PP0068	PP0056	Security Target
OT.Data_Integrity	X		(E)
OT.Data_Authenticity	X		(E)
OT.Data_Confidentiality	X		(E)
OT.Tracing	X		(E)
OT.Prot_Abuse-Func	X		(E)
OT.Prot_Inf_Leak	X		(E)
OT.Prot_Phys-Tamper	X		(E)
OT.Prot_Malfunction	X		(E)
OT.Identification	X		(E)
OT.AC_Pers	X		(E)
OT.Sens_Data_Conf		X	(E)
OT.Chip_Auth_Proof		X	(E)
OT.Active_Authentication			(A)

Table 10 Security objectives for the TOE Consistency table

2.4.3.2 Objective for Environment consistency

All Security Objectives for the Operational Environment defined in [PP0056] and [PP0068] are relevant for the TOE of this Security Target. The table below indicates the Objective for Environment consistency and the additions.

O.ENV	PP0068	PP0056	Security Target
OE.Legislative_Compliance	X		(E)
OE.Passive_Auth_Sign	X		(E)
OE.Personalisation	X		(E)
OE.Terminal	X		(E)
OE.Travel_Document_Holder	X		(E)
OE.Auth_Key_Travel_Document		X	(E)
OE.Authoriz_Sens_Data		X	(E)

OE.Exam_Travel_Document		X	(E)
OE.Prot_Logical_Travel_Document		X	(E)
OE.Ext_Insp_Systems		X	(E)
OE.Active_Auth-Sign			(A)
OE.Active_Auth-Verif			(A)

Table 11 Security objectives for the OE Consistency table

2.4.4 Conformity of the Requirement (SFR/SAR)

2.4.4.1 SFR consistency

Several SFRs from [PP0056] and [PP0068] have been adapted in this ST as BSI-CC-PP-0056 and BIS-CC-PP-0068 claim conformance to CC Version 3.1, Revision 2, and this ST claims to CC:2022, Revision 1. CC:2022, Revision 1 has already included new SFRs and has modified the instantiation of some SFRs.

SFR	PP0068	PP0056	Security Target
FAU_SAS.1	X		(E)
FCS_CKM.1/CA Key pair			(A)
FCS_CKM.1/AA			(A)
FCS_CKM.1/DH_PACE	X		(E)
FCS_CKM.1/CA		X	(E)
FCS_CKM.4	X		(M)
FCS_CKM.6			(M)
FCS_COP.1/PACE_ENC	X		(E)
FCS_COP.1/PACE_MAC	X		(E)
FCS_COP.1/CA_ENC		X	(E)
FCS_COP.1/SIG_VER		X	(E)
FCS_COP.1/CA_MAC		X	(E)
FCS_COP.1/AA			(A)
FCS_RND.1	X		(M)
FCS_RNG.1			(M)
FIA_AFL.1/PACE	X		(E)
FIA_UID.1/PACE		X	(E)
FIA_UAU.1/PACE		X	(E)
FIA_UAU.4/PACE		X	(E)
FIA_UAU.5/PACE		X	(E)
FIA_UAU.6/PACE	X		(E)
FIA_UAU.6/EAC		X	(E)
FIA_API.1		X	(R)
FIA_API.1/AA			(A)
FDP_ACC.1/TRM		X	(E)
FDP_ACF.1/TRM		X	(E)

FDP_RIP.1	X		(E)
FDP_UCT.1/TRM	X		(E)
FDP_UIT.1/TRM	X		(E)
FTP_ITC.1/PACE	X		(E)
FDP_ITC.1/CA			(A)
FDP_ITC.1/AA			(A)
FDP_ITC.1/PERSO KEY			(A)
FMT_SMF.1	X		(E)
FMT_SMR.1/PACE		X	(E)
FMT_LIM.1		X	(E)
FMT_LIM.2		X	(E)
FMT_MTD.1/INI_ENA	X		(E)
FMT_MTD.1/INI_DIS	X		(E)
FMT_MTD.1/CVCA_INI		X	(E)
FMT_MTD.1/CVCA_UPD		X	(E)
FMT_MTD.1/DATE		X	(E)
FMT_MTD.1/CAPK		X	(E)
FMT_MTD.1/AAK			(A)
FMT_MTD.1/KEY_READ		X	(R)
FMT_MTD.1/PA	X		(E)
FMT_MTD.3		X	(E)
FPT_EMS.1		X	(R)
FPT_FLS.1	X		(E)
FPT_TST.1	X		(E)
FPT_PHP.3	X		(E)

Table 12 SFR Consistency table

- (1) The **FCS_CKM.1/CA Key pair** is added to follow the requirement by the **FMT_MTD.1/CAPK**.
- (2) The **FCS_CKM.4** is deprecated in the [CC:2022 P2], and replaced by **FCS_CKM.6**.
- (3) The **FCS_RND.1** is in the Extended Components Definition part in the [PP0068], it is replaced by **FCS_RNG.1** in [CC:2022 P2].
- (4) The **FIA_API.1** is in the Extended Components Definition part in the [PP0056], it is refined according to [CC:2022 P2].
- (5) The **FMT_LIM.1** and **FMT_LIM.2** are in the Extended Components Definition part in the [PP0056], they are included in [CC:2022 P2].
- (6) The **FPT_EMS.1** is in the Extended Components Definition part in the [PP0068], it is refined according to [CC:2022 P2].
- (7) The **FMT_MTD.1/KEY_READ** is refined to cover **OT.Active_Authentication**.
- (8) The **FCS_CKM.1/AA**, **FCS_COP.1/AA**, **FIA_API.1/AA**, **FDP_ITC.1/AA** and **FMT_MTD.1/AAK** are added to cover **OT.Active_Authentication**.
- (9) The **FDP_ITC.1/CA** is added to cover the loading of Chip Authentication Private Key.
- (10) The **FDP_ITC.1/PERSO KEY** is added to cover the replacing of Personalization Agent Key.

3 Security Problem Definition

3.1 Introduction

The definition of Assets and Subjects from [PP0056] and [PP0068] is not presented here. The complete list for the Assets and Subjects is in the section 2.4.2.1 and section 2.4.2.2.

3.2 Assumptions

The definition of Assumptions from [PP0056] and [PP0068] is not presented here. The complete list for the Assumptions is in the section 2.4.2.3.

3.3 Threats

The definition of Threats from [PP0056] and [PP0068] is not presented here. The complete list for the Threats is in the section 2.4.2.4.

3.4 Organizational Security Policies

The definition of OSPs from [PP0056] and [PP0068] is not presented here. The complete list for the OSPs is in the section 2.4.2.5.

4 Security Objectives

This section introduces the security objectives for the TOE.

4.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP0056] and [PP0068] are not repeated here. See section 2.4.3.1 for Security Objectives for the TOE.

Added Security Objectives for the TOE description is detailed below:

OT.Active_Authentication Proof of MRTD's chip authenticity through AA

The TOE must support the BIS to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO9303]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

4.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the Operational Environment from [PP0056] and [PP0068] are not repeated here. See section 2.4.3.2 for Security Objectives for the Operational Environment.

Added Security Objectives for the Operational Environment description is detailed below:

OE.Active_Auth-Sign Active Authentication of logical MRTD by Signature

The issuing State or Organization must

- (1) generate the Active Authentication Key Pair,
- (2) ensure the secrecy of the Active Authentication Private Key, sign and store the Active Authentication Public Key in EF.DG15 and
- (3) support the inspection system to verify the authenticity of the Active Authentication public key through Passive authentication.

OE.Active_Auth-Verif Verification by Active Authentication

The inspection systems verify the AA digital signature by active authentication, which can ensure the data are read from the genuine contactless IC and that the contactless IC and physical document belong to each other.

4.3 Security Objectives Rationale

4.3.1 Rationale between Objectives and SPD

The security objectives rationale from [PP0056] and [PP0068] is not presented here. Added rationales is detailed below:

	OT.Active_Authentication	OT.Chip_Auth_Proof	OE.Active_Auth_Sign	OE.Active_Auth_Verif	OE.Auth_Key_Travel_Document	OE.Exam_Travel_Document
T.Counterfeit	X	X	X	X	X	X

Table 13 Security Objective Rationale

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 an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** “Travel document Authentication Key”. According to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document’s chip.

The threat **T.Counterfeit** 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_Authentication** using an Active Authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Document Security Objects as demanded by **OE.Active_Auth-Sign**. According to **OE.Active_Auth-Verif** the Basic Inspection system has to perform the Active Authentication Protocol to verify the authenticity of the travel document’s chip.

OE.Active_Auth-Sign and OE.Active_Auth-Verif can be added to the objectives defined in the [PP0056] and [PP0068]. The OE.Active_Auth-Sign and OE.Active_Auth-Verif neither mitigates the T.Counterfeit addressed by OT.Chip_Auth_Proof nor fulfils any OSPs.

Justification:

- (1) OE.Active_Auth-Sign and OE.Active_Auth-Verif together require another mechanism for verifying the authenticity of chips, completely different from Chip Authentication which described by OT.Chip_Auth_Proof.
- (2) Specifically, OE.Active_Auth-Sign requests the management of Active Authentication key pair used for Active Authentication, the Active Authentication key pair and Chip Authentication key pair are two different keys, stored in separate EF files and do not affect each other.

- (3) The OE.Active_Auth-Verif requires the signature verification operation by the inspection system in accordance to Active Authentication protocol, while the Chip Authentication described by OT.Chip_Auth_Proof requires an ephemeral-static Diffie-Hellman key agreement protocol.
- (4) The OE.Active_Auth-Sign and OE.Active_Auth-Verif do not fulfils any OSPs addressed by security objectives for the TOE.

4.3.2 Compatibility between Objectives of the TOE and [TMC_IC]

4.3.2.1 Objectives for the TOE

Compatibility between Objectives of the TOE and [TMC_IC] is mapped below, and the notation used is detailed below:

- Compatible(C): The element is specific to this ST and does not conflict with the [TMC_IC].
- Included (I): The element is this ST is also included in the [TMC_IC].

Objectives for TOE	[TMC_IC]	Security Target
OT.Data_Integrity		(C)
OT.Data_Authenticity		(C)
OT.Data_Confidentiality		(C)
OT.Tracing		(C)
OT.Prot_Abuse-Func	X	(I): Included in O.Abuse-Func
OT.Prot_Inf_Leak	X	(I): Included in O.Leak-Inherent
OT.Prot_Phys-Tamper	X	(I): Included in O.Phys-Manipulation and O.Phys-Probing
OT.Prot_Malfunction	X	(I): Included in O.Malfunction
OT.Identification	X	(I)
OT.AC_Pers		(C)
OT.Sens_Data_Conf		(C)
OT.Chip_Auth_Proof		(C)
OT.Active_Authentication		(C)

Table 14 Objectives for the TOE and [TMC_IC] compatibility table

We can therefore conclude that the objectives for the TOE of this ST and [TMC_IC] are consistent.

4.3.2.2 Objectives for the Operational Environment

The following table shows the compatibility between the objectives for the operational environment of the TOE and [TMC_IC], and they are separated into three groups:

- IrOE: The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the base component.

- CfPOE: The objectives for the environment being fulfilled by the Composite-ST automatically. Such objectives of the environment of the base-ST can always be assigned to the TOE security objectives of the Composite-ST. Due to this fact they will be fulfilled either by the Composite product-SFR or by the Composite-SAR automatically.
- SgOE: The remaining Objectives for the environment of the base-ST belonging neither to the group IrOE nor CfOE Exactly this group makes up the significant objectives for the environment for the Composite-ST, which shall be addressed in the Composite-ST.

Objectives for the OE from the [TMC_IC]	IrOE	CfPOE	SgOE
OE.Resp-Appl		X	
OE.Process-Sec-IC			X

Table 15 Objectives for OE compatibility table

We can therefore conclude that the objectives for the OE of this ST and [TMC_IC] are consistent.

5 Extended Components Definition

5.1 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 data storage

5.1.1 Family behavior

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

5.1.2 Component leveling and description

Figure 1 shows the component leveling for this family.

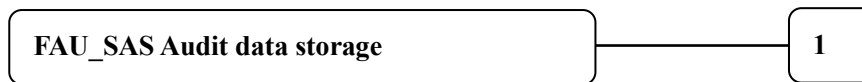


Figure 3 FAU_SAS: Component leveling

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

5.1.3 Management of FAU_SAS.1

There are no management activities foreseen.

5.1.4 Audit of FAU_SAS.1

There are no actions defined to be auditable.

5.1.5 FAU_SAS.1 Audit storage

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SAS.1.1

The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

6 Security Requirements

The definition of the SFR uses the following typographical convention:

- ***Bold italic text is used for assignments and selections performed by the ST writer.***
- **Underlined bold text is used for assignments and selections performed by the PP author.**
- *Underlined italic text is used for refinements performed by the ST writer.*
- Iterations are indicated by appending a termination of the form ‘/ITERATION TAG’ to the corresponding component. For instance: FDP_ITC.1/PERSO KEY, FDP_ITC.1/AA.

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 8 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC:2022 P2]. The operation “load” is synonymous to “import” used in [CC:2022 P2].

Definition of security attributes:

Security attribute	Values	Meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR03110-1]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR03110-1]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR03110-1]); Terminal is

		authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [TR03110-1]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR03110-1])
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR03110-1])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [TR03110-1])
CA session keys	Present/Absence	Both the IC and the terminal derive the CA session keys for secure messaging.
AA digital signature	Present/Absence	Generated by the IC and provide to external entity in accordance with the definition of FIA_API.1/AA.

Table 16 Definition of security attributes

The following table provides an overview of the keys and certificates used.

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a

	domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR03110-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC} , PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [ISO 11770-3].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document

	Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

Table 17 Overview of the keys and certificates

The following table lists the SFRs that are copied directly from the [PP0056] and [PP0068], all assignments and selections operations are taken as defined in the [PP0056] and [PP0068]. These SFRs are not presented in this ST.

Security functional requirement	Title	PP0068	PP0056
FAU_SAS.1	Audit storage	X	
FIA_UAU.6/PACE	Re-authenticating of Terminal by the TOE	X	
FIA_UAU.6/EAC	Re-authenticating of Terminal by the TOE		X
FDP_ACC.1/TRM	Subset access control		X
FDP_ACF.1/TRM	Security attribute-based access control		X
FDP_UIT.1/TRM	Data exchange integrity	X	
FDP_UCT.1/TRM	Basic data exchange confidentiality – MRTD	X	
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE	X	
FMT_SMF.1	Specification of Management Functions	X	
FMT_SMR.1/PACE	Security roles		X
FMT_LIM.1	Limited capabilities		X
FMT_LIM.2	Limited availability		X
FMT_MTD.1/INI_ENA	Management of TSF data – Writing Initialization and Pre-personalization Data	X	

FMT_MTD.1/INI_DIS	Management of TSF data – Reading and Using Initialization and Pre-personalization Data	X	
FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifying Certification Authority		X
FMT_MTD.1/DATE	Management of TSF data – Current date		X
FMT_MTD.1/PA	Management of TSF data – Personalization Agent	X	
FMT_MTD.3	Secure TSF data		X
FPT_PHP.3	Resistance to physical attack	X	

Table 18 SFR list

6.1 Security Functional Requirements

6.1.1 Class FCS Cryptographic Support

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/CA Key pair - Cryptographic key generation for CA

FCS_CKM.1.1/CA Key pair

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Following algorithm* and specified cryptographic key sizes *Following key size* that meet the following: *standard*.

Algorithm	Key Size	Standard
<i>ECDH Key generation</i>	<i>BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384 and NIST P-521</i>	<i>[TR03111] [SP800-186]</i>

Table 19 FCS_CKM.1/CA Key pair explanation

FCS_CKM.1/AA Cryptographic key generation for AA

FCS_CKM.1.1/AA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Following algorithm* and specified cryptographic key sizes *Following key size* that meet the following: *standard*.

Algorithm	Key Size	Standard
-----------	----------	----------

<i>ECC Key generation</i>	<i>BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384 and NIST P-521</i>	<i>[TR03111] [SP800-186]</i>
<i>RSA-CRT key generation</i>	<i>2048, 3072 and 4096 bits</i>	<i>[PKCS1]</i>

Table 20 FCS_CKM.1/AA explanation

Application note: The keys size 2048 for RSA-CRT algorithm is supported by the product but has legacy until December 2025 with [ACM]. Therefore, its usage from the mentioned date and on is not recommended.

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

FCS_CKM.1.1/DH_PACE

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *see selection (Algorithm) in table below* and specified cryptographic key sizes *see assignment (Key Size) in table below* that meet the following: **[SAC]**.

Algorithm	Key Size
<i>ECDH compliant to [TR03111]</i>	<i>192 and 256 bits</i>
<i>Diffie-Hellman-Protocol compliant to [PKCS3]</i>	<i>192 and 256 bits</i>

Table 21 FCS_CKM.1/DH_PACE explanation

Application note: The key size for the intermediate keys in the DH protocol is 2048 bits. The key sizes for the intermediate keys in the ECHD protocol are 256, 384, 512 and 521 bits. The values shown in the “Key Size” column in the table above are for the resulting (AES) session keys.

Application note: The keys size 2048 for the intermediate keys in the DH Key Agreement algorithm is supported by the product but has legacy until December 2025 with [ACM]. Therefore, its usage from the mentioned date and on is not recommended.

Application note: The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [SAC]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [PKCS3]) or on the ECDH compliant to TR03111 (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [SAC] and [TR03111] for details). The shared secret value *K* is used for deriving the AES session keys for message encryption and message authentication (PACE-*K*_{MAC}, PACE-*K*_{ENC}) according to [SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application note: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [SAC].

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

FCS_CKM.1.1/CA

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *see assignment (Algorithm) in table below* and specified cryptographic key sizes *see assignment (Key Size) in table below* that meet the following: *see selection (Standard) in table below*.

Algorithm	Key Size	Standard
<i>AESSession-DH Key Agreement Algorithm – PKCS#3 – 2048 bits</i>	<i>192 and 256 bits</i>	<i>based on the Diffie-Hellman key derivation protocol compliant to [PKCS3] and [TR03110-1]</i>
<i>AESSession-ECDH Key Agreement Algorithm – ISO 15946 – 256, 384, 512 and 521 bits</i>	<i>192 and 256 bits</i>	<i>based on an ECDH protocol compliant to [TR03111]</i>

Table 22 FCS_CKM.1/CA explanation

Application note: The keys size 2048 for DH Key Agreement algorithm is supported by the product but has legacy until December 2025 with [ACM]. Therefore, its usage from the mentioned date and on is not recommended.

Application note: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [TR03110-1].

Application note: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [TR03110-1]. This protocol may be based on the Diffie- Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [PKCS3]) or on the ECDH compliant to TR03111 (i.e. an elliptic curve cryptography algorithm) (cf. [TR03111], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [TR03110-1]).

Application note: The TOE shall destroy any session keys in accordance with FCS_CKM.6 after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.6 is also fulfilled by FCS_CKM.1/CA.

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.6)” as specified below (Common Criteria Part 2).

FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_CKM.6.1

The TSF shall destroy *following cryptographic keys (including keying material)* when *following scenario*.

Cryptographic keys	Scenario
<i>Ephemeral PACE private key</i>	(1) <i>For the private key used in GM and IM mapping, immediately after deriving the shared secret.</i> (2) <i>For the private key used in CAM mapping, immediately after calculation of CA_{IC}.</i> (3) <i>For the private key used in key agreement, immediately after deriving the shared secret</i>
<i>PACE derivation data</i>	<i>Immediately after deriving the shared secret</i>
<i>PACE session Keys</i>	(1) <i>A Secure Messaging error occurs</i> (2) <i>A plain APDU is received</i> (3) <i>After generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys.</i>
<i>CA session Keys</i>	(1) <i>A Secure Messaging error occurs</i> (2) <i>A plain APDU is received</i> (3) <i>After successful run of the Chip Authentication Protocol</i>
<i>PACE shared secret K</i>	<i>Immediately after deriving the PACE session keys</i>
<i>CA shared secret K</i>	<i>Immediately after deriving the CA session keys</i>
<i>Personalization session keys</i>	(1) <i>The on-card Application Session is terminated.</i> (2) <i>The associated logical channel is explicitly closed.</i> (3) <i>The card is reset, deactivated or powered off: i.e. the Card Session ends</i>

Table 23 FCS_CKM.6.1 explanation

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *following cryptographic key destruction method* that meets the following: *following standard*.

Cryptographic keys	Destruction methods	Standard
<i>Ephemeral PACE private key</i>	<i>Clearing with random number</i>	<i>none</i>
<i>PACE derivation data</i>	<i>Clearing with random number</i>	<i>none</i>

<i>PACE session Keys</i>	<i>Clearing with random number</i>	<i>none</i>
<i>CA session Keys</i>	<i>Clearing with random number</i>	<i>none</i>
<i>PACE shared secret K</i>	<i>Clearing with random number</i>	<i>none</i>
<i>CA shared secret K</i>	<i>Clearing with random number</i>	<i>none</i>
<i>Personalization session keys</i>	<i>Clearing with random number</i>	<i>none</i>

Table 24 FCS_CKM.6.2 explanation

Application note: The PACE derivation data includes the PACE ephemeral domain parameters and nonce.

Application note: The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

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/PACE_ENC Cryptographic operation – Encryption / Decryption AES

FCS_COP.1.1/PACE_ENC

The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: **compliant to [SAC]**.

Algorithm	Key Size
<i>AES in CBC mode</i>	<i>192 and 256 bits</i>

Table 25 FCS_COP.1/PACE_ENC explanation

Application note: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{ENC}).

FCS_COP.1/PACE_MAC Cryptographic operation – MAC

FCS_COP.1.1/PACE_MAC

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: **compliant to [SAC]**.

Algorithm	Key Size
<i>AES CMAC</i>	<i>192 and 256 bits</i>

Table 26 FCS_COP.1/PACE_MAC explanation

Application note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}).

FCS COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption

FCS_COP.1.1/CA_ENC

The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: *following standards*.

Algorithm	Key Size	Standard
<i>AES in CBC mode</i>	<i>192 and 256 bits</i>	<i>[FIPS 197]</i>

Table 27 FCS_COP.1/CA_ENC explanation

Application note: This SFR requires the TOE to implement the cryptographic primitives (e.g. AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

FCS COP.1/SIG_VER Cryptographic operation – Signature verification by travel document

FCS_COP.1.1/SIG_VER

The TSF shall perform **digital signature verification** in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: *following standards*.

Algorithm	Key Size	Standard
<i>RSA-CRT</i>	<i>2048 and 3072 bits</i>	<i>RSA-PSS in [PKCS1]</i>
<i>ECC</i>	<i>BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256 and NIST P-384</i>	<i>[ICAO9303]</i>

Table 28 FCS_COP.1/SIG_VER explanation

Application note: The keys size 2048 for RSA-CRT algorithm is supported by the product but has legacy until December 2025 with [ACM]. Therefore, its usage from the mentioned date and on is not recommended.

FCS_COP.1/CA_MAC Cryptographic operation – MAC

FCS_COP.1.1/CA_MAC

The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: *following standards*.

Algorithm	Key Size	Standard
<i>AES CMAC</i>	<i>192 and 256 bits</i>	<i>[NIST-800-38B]</i>
<i>AES</i>	<i>128 bits</i>	<i>[FIPS 197]</i>

Table 29 FCS_COP.1/CA_MAC explanation

Application note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore, the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

FCS_COP.1/AA Cryptographic operation – Active Authentication

FCS_COP.1.1/AA

The TSF shall perform *digital signature creation* in accordance with a specified cryptographic *following algorithm* and cryptographic key sizes *following key size* that meet the following: *following standards*.

Algorithm	Key Size	Standard
<i>RSA-CRT</i>	<i>2048, 3072 and 4096 bits</i>	<i>[ISO 9796-2]</i>
<i>ECDSA</i>	<i>BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384 and NIST P-521</i>	<i>[TR03111] [SP800-186]</i>

Table 30 FCS_COP.1/AA explanation

Application note: The keys size 2048 for RSA-CRT algorithm is supported by the product but has legacy until December 2025 with [ACM]. Therefore, its usage from the mentioned date and on is not recommended.

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RNG.1)” as specified below (Common Criteria Part 2).

FCS_RNG.1 Random number generation

FCS_RNG.1.1

The TSF shall provide a *physical* random number generator that implements:

- *A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
- *If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*
- *The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started. And (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
- *The online test procedure shall be effective to detect non-tolerable weakness of the random numbers soon.*
- *The online test procedure checks the quality of the raw random number sequence. It is triggered applied upon specified internal events. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time*

FCS_RNG.1.2

The TSF shall provide *32-bit random number words* that meet:

- *Test procedure A and no other test suites does not distinguish the internal random numbers from output sequences of an ideal RNG.*
- *The average Shannon entropy per internal random bit exceeds 0.997.*

Application note: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols (PACE) as required by FIA_UAU.4/PACE.

6.1.2 Class FIA Identification and Authentication

Application note: The following table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication Protocol	FIA_API.1/AA

Table 31 Overview on authentication SFR

Note the Chip Authentication Protocol Version 1 as defined in this Security Target includes:

the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,

the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

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

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorization data

FIA_AFL.1.1/PACE

The TSF shall detect when *following positive integer number* unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password**.

Positive integer number
1

Table 32 FIA_AFL.1.1/PACE explanation

FIA_AFL.1.2/PACE

When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall *following actions*.

Actions
<i>Exponentially increasing time delay before new authentication attempt is possible</i>

Table 33 FIA_AFL.1.2/PACE explanation

Application note: The formulation of the delay time is in the following. ‘t’ is the delay time (ms), and ‘n’ is the unsuccessful authentication attempt.

$$t=100 \cdot 2^{n-1}$$

Application Note: Since all non-blocking authorization data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy, the TOE shall not allow a quick monitoring of its behavior (e.g. due to a long reaction time) in order to make the first step of the skimming attack requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current ST.

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

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE

The TSF shall allow

- 1. to establish the communication channel,**
- 2. carrying out the PACE Protocol according to [SAC],**
- 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,**
- 4. to carry out the Chip Authentication Protocol v.1 according to [TR03110-1],**
- 5. to carry out the Terminal Authentication Protocol v.1 according to [TR03110-1],**
- 6. to carry out the Active Authentication according to [ICA09303]**

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

FIA_UID.1.2/PACE

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

Application note: In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. 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 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization Agent Key).

Application note: User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorized other person or device (Basic Inspection System with PACE).

Application note: In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC.

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

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE

The TSF shall allow

- 1. to establish the communication channel,**

- 2. carrying out the PACE Protocol according to [SAC],**
- 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,**
- 4. to identify themselves by selection of the authentication key,**
- 5. to carry out the Chip Authentication Protocol Version 1 according to [TR03110-1],**
- 6. to carry out the Terminal Authentication Protocol Version 1 according to [TR03110-1],**
- 7. to carry out the Active Authentication Protocol according to [ICA09303]**

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

FIA_UAU.1.2/PACE

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

Application note: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorized other person or device (BIS-PACE).

If PACE was successfully performed, secure messaging is started using the derived session keys (PACE- K_{MAC} , PACE- K_{ENC}), cf. FTP_ITC.1/PACE.

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

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

FIA_UAU.4.1/PACE

The TSF shall prevent reuse of authentication data related to

- 1. PACE Protocol according to [SAC],**
- 2. Authentication Mechanism based on AES,**
- 3. Terminal Authentication Protocol v.1 according to [TR03110-1].**

The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [PP0068].

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 Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

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

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE

The TSF shall provide

- 1. PACE Protocol according to [SAC],**
- 2. Passive Authentication according to [ICA09303],**

- 3. Secure messaging in MAC-ENC mode according to [SAC],
 - 4. Symmetric Authentication Mechanism based on AES,
 - 5. Terminal Authentication Protocol v.1 according to [TR03110-1]
- to support user authentication.

FIA_UAU.5.2/PACE

The TSF shall authenticate any user's claimed identity according to the

- 1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
- 2. The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key(s).
- 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
- 4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2).

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1

The TSF shall provide a **Chip Authentication Protocol Version 1 according to [TR03110-1]** to prove the identity of **TOE** by including the following properties *CA session keys* to an external entity.

Application note: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR03110-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO9303]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication proof of identity – Active Authentication

FIA_API.1.1/AA

The TSF shall provide an *Active Authentication Protocol according to [ICAO9303]* to prove the identity of **TOE** by including the following properties *AA Digital signature* to an external entity.

6.1.3 Class FDP User Data Protection

The TOE shall meet the requirement "Subset residual information protection (FDP_RIP.1)" as specified below (Common Criteria Part 2)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

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

- 1. Session Keys (immediately after closing related communication session),**
- 2. the ephemeral private key $ephem - SK_{P_{ICC}}$ - PACE (by having generated a DH shared secret K).**

Application note: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.6 that merely requires a fact of key destruction according to a method/standard.

The TOE shall meet the requirements of "Import of user data without security attributes (FDP_ITC.1)" as specified below (Common Criteria Part 2).

FDP_ITC.1/PERSO KEY Import of user data without security attributes – Personalization Agent Key

FDP_ITC.1.1

The TSF shall enforce the *Access Control SFP* when *replacing the Personalization Agent Key*, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *The Personalization Agent shall authenticate itself by presenting the previous version of the Personalization Agent Key before being granted permission to replace it.*

Application note: This SFR models the requirements for importing the Personalization Agent Key by a successfully authenticated Personalization Agent. This allows the Personalization Agent to replace the original Personalization Agent Key, loaded by the Manufacturer before delivery, with their own securely generated Personalization Agent Key. Moreover, it prevents any entity not provided with the current Personalization Agent Key from replacing it and, by extension, from being able to assume the role of the Personalization Agent.

Application note: from the point of view of the TOE Life Cycle, Personalization Agent and Pre-personalization Agent (i.e. MRTD Manufacturer) constitute differentiated roles. However, in the scope of this SFR, the term "Personalization Agent" is used collectively for both roles, as the authentication mechanism for both is the same. Optionally, it is up to the MRTD Manufacturer to modify the default Personalization Agent Key from the default value – in this case, it would be the responsibility of the MRTD Manufacturer to share the new value of the Personalization Agent Key with the Personalization Agent in a secure way which preserves confidentiality. Likewise, it is up to the Personalization Agent to modify the value of the Personalization Agent Key, either from the default value (if it was not modified by the MRTD Manufacturer) or from the new value set by the MRTD Manufacturer.

FDP_ITC.1/CA Import of user data without security attributes – Chip Authentication Key

FDP_ITC.1.1

The TSF shall enforce the *Access Control SFP* when loading the Chip Authentication keys, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *the terminal successfully authenticate itself as Personalization Agent by presenting the Personalization Agent Key*.

FDP_ITC.1/AA Import of user data without security attributes – Active Authentication Key**FDP_ITC.1.1**

The TSF shall enforce the *Access Control SFP* when loading the Active Authentication keys, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *the terminal successfully authenticate itself as Personalization Agent by presenting the Personalization Agent Key*.

6.1.4 Class FMT Security Management

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/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date**FMT_MTD.1.1/CVCA_INI**

The TSF shall restrict the ability to write the

1. initial Country Verifying Certification Authority Public Key,

2. initial Country Verifying Certification Authority Certificate,

3. initial Current Date

to *the Personalization Agent*.

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key**FMT_MTD.1.1/CAPK**

The TSF shall restrict the ability to *create and load* the Chip Authentication Private Key to *the Personalization Agent*.

Application note: The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Active Authentication Private Key is generated by the TOE itself. The TOE supports both methods for importing the Chip Authentication Private Key.

FMT_MTD.1/AAK Management of TSF data – Active Authentication Private key

FMT_MTD.1.1/AAK

The TSF shall restrict the ability to *create and load* the *Active Authentication Private Key* to *Personalization Agent*.

Application note: The TOE supports the creation and loading of RSA-CRT private key, as well as creation and loading of ECC private key.

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

FMT_MTD.1.1/KEY_READ

The TSF shall restrict the ability to read the

1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalization Agent Keys,
4. Active Authentication Private Key

to none.

6.1.5 Class FPT Protection of the Security Functions

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

The TOE shall meet the requirement “TOE Emanation (FPT_EMS.1)” as specified below (Common Criteria Part 2).

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1

The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in the following table:

ID	Emissions	Attack surface	TSF data	User data
----	-----------	----------------	----------	-----------

1	<i>Electromagnetic emissions</i>	<i>Any</i>	<u>1. Chip Authentication Session Keys</u> <u>2. PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC}),</u> <u>3. the ephemeral private key ephem SK_{PICC}-PACE,</u> <u>4. Personalization Agent Key(s)</u> <u>5. Chip Authentication Private Key</u> <u>6. Active Authentication Private Key</u> <u>7. EF.SOD</u>	<i>EF.DG1-DG16</i> <i>EF.COM</i> <i>EF.CardSecurity</i> <i>EF.CVCA</i>
2	<i>Current emissions</i>	<i>Smart card circuit contacts</i>		

Table 34 FPT_EMS.1.1 table

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

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:

- 1. Exposure to operating conditions causing a TOE malfunction,**
- 2. Failure detected by TSF according to FPT_TST.1.**

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

FPT_TST.1 TSF testing

FPT_TST.1.1

The TSF shall run a suite of self-tests *before any operation on key data* to demonstrate the correct operation of **the TSF.**

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of **TSF data.**

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of **stored TSF executable code.**

Application note: The FPT_TST.1.2 and FPT_TST.1.3 are fulfilled by the memory redundancy security function provided by certified IC. All data stored in memories has redundant bits, which prevent attacker from modifying the values in memory.

6.2 Security Assurance Requirements

The Security Assurance Requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) as defined in [CC:2022 P5], and the Composite Product Package (COMP) as defined in [CC:2022 P5].

And augmented by taking the following component

- ALC_DVS.2
- ALC_FLR.1 and
- AVA_VAN.5

6.3 Security Requirements Rationale

6.3.1 Dependency Rationale

6.3.1.1 SFR Dependency

SFR	Dependencies	ST dependencies
FAU_SAS.1	No dependencies	N/A
FCS_CKM.1/CA Key Pair	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC Justification 1 for non-satisfied dependencies FCS_CKM.3, see section 6.3.1.2 Fulfilled by FCS_RNG.1 Justification 2 for non-satisfied dependencies FCS_CKM.6, see section 6.3.1.2
FCS_CKM.1/AA	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access	Fulfilled by FCS_COP.1/AA Justification 1 for non-satisfied dependencies FCS_CKM.3, see section 6.3.1.2 Fulfilled by FCS_RNG.1 Justification 2 for non-satisfied dependencies FCS_CKM.6, see section 6.3.1.2

	[FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	Fulfilled by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC Justification 1 for non-satisfied dependencies FCS_CKM.3, see section 6.3.1.2 Fulfilled by FCS_RNG.1 Fulfilled by FCS_CKM.6
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC Justification 1 for non-satisfied dependencies FCS_CKM.3, see section 6.3.1.2 Fulfilled by FCS_RNG.1 Fulfilled by FCS_CKM.6
FCS_CKM.6	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/PACE_ENC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	Fulfilled by FCS_CKM.1/DH_PACE

	FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2
FCS_COP.1/PACE_MAC	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Fulfilled by FCS_CKM.1/DH_PACE Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2
FCS_COP.1/CA_ENC	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Fulfilled by FCS_CKM.1/CA Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2
FCS_COP.1/CA_MAC	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Fulfilled by FCS_CKM.1/CA and FDP_ITC.1/PERSO KEY Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2
FCS_COP.1/SIG_VER	[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, or FCS_CKM.5 Cryptographic key derivation]	Fulfilled by FCS_CKM.1/CA Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2

	FCS_CKM.3 Cryptographic key access	
FCS_COP.1/AA	[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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Fulfilled by FCS_CKM.1/AA Justification 1 for non-satisfied dependencies FCS_CKM.3 , see section 6.3.1.2
FCS_RNG.1	No dependencies	N/A
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	N/A
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	N/A
FIA_UAU.5/PACE	No dependencies	N/A
FIA_UAU.6/PACE	No dependencies	N/A
FIA_UAU.6/EAC	No dependencies	N/A
FIA_API.1	No dependencies	N/A
FIA_API.1/AA	No dependencies	N/A
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute-based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute	Fulfilled by FDP_ACC.1/TRM Justification 3 for non-satisfied dependencies FMT_MSA.3 , see section 6.3.1.2
FDP_RIP.1	No dependencies	N/A
FDP_UCT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1/TRM Fulfilled by FTP_ITC.1/PACE
FDP_UIT.1/TRM	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1/TRM Fulfilled by FTP_ITC.1/PACE

	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	
FTP_ITC.1/PACE	No dependencies	N/A
FDP_ITC.1/PERSO KEY	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM Justification 4 for non-satisfied dependencies FMT_MSA.3 , see section 6.3.1.2
FDP_ITC.1/AA	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM Justification 4 for non-satisfied dependencies FMT_MSA.3 , see section 6.3.1.2
FDP_ITC.1/CA	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM Justification 4 for non-satisfied dependencies FMT_MSA.3 , see section 6.3.1.2
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2 Limited availability	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1 Limited capabilities	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/INI_DIS	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/CVCA_INI	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/CVCA_UPD	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1

FMT_MTD.1/DATE	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/CAPK	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/AAK	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/KEY_READ	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.1/PA	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1/PACE Fulfilled by FMT_SMF.1
FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	N/A
FPT_FLS.1	No dependencies	N/A
FPT_TST.1	No dependencies	N/A
FPT_PHP.3	No dependencies	N/A

Table 35 SFR Dependencies

6.3.1.2 Justification for non-satisfied dependencies

No.	SFR	Justification for non-satisfied dependencies
1	FCS_CKM.1/CA Key Pair, FCS_CKM.1/AA, FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/SIG_VER, FCS_COP.1/AA	The TOE does not provide any key access methods. Once keys are generated (FCS_CKM.1), the use of key is incorporated with cryptographic operation (FCS_COP.1), which is not considered as key access (FCS_CKM.3). Thus, there is no necessity for FCS_CKM.3 .
2	FCS_CKM.1/CA Key	The SFR FCS_CKM.1/CA Key Pair and FCS_CKM.1/AA uses the

	Pair, FCS_CKM.1/AA	asymmetric key generated or imported during the Personalization process (cf. FMT_MTD.1/CAPK and FMT_MTD.1/AAK) by the personalization agent. Since the key is permanently stored within the TOE there is no need for FCS_CKM.6 .
3	FDP_ACF.1/TRM	The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here. (see [PP0068])
4	FDP_ITC.1/PERSO KEY, FDP_ITC.1/AA FDP_ITC.1/CA	The dependency between FDP_ITC.1 and FMT_MSA.3 refers to the values of security attributes assigned by default to the user data imported through FDP_ITC.1 . However, in the case of FDP_ITC.1/PERSO KEY , FDP_ITC.1/AA and FDP_ITC.1/CA , the imported user data (the Personalization Key, the Active Authentication Key and the Chip Authentication Key, respectively) have no associated security attributes. Therefore, static attribute initialization as defined by FMT_MSA.3 is not applicable in this case.

Table 36 Non-satisfied Dependencies

6.3.1.3 SAR Dependency

SAR	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_IMP.1, ADV_TDS.1	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.3, ALC_TAT.1	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5	ADV_FSP.5
ADV_COMP.1	No Dependencies	No Dependencies
AGD_OPE.1	ADV_FSP.1	ADV_FSP.5
AGD_PRE.1	No Dependencies	No Dependencies
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	No Dependencies
ALC_DEL.1	No Dependencies	No Dependencies
ALC_DVS.2	No Dependencies	No Dependencies
ALC_FLR.1	No Dependencies	No Dependencies
ALC_LCD.1	No Dependencies	No Dependencies
ALC_TAT.2	ADV_IMP.1	ADV_IMP.1
ALC_COMP.1	No Dependencies	No Dependencies
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	No Dependencies

ASE_INT.1	No Dependencies	No Dependencies
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	No Dependencies
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2, ADV_FSP.5
ASE_COMP.1	No Dependencies	No Dependencies
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_COMP.1	No Dependencies	No Dependencies
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3
AVA_COMP.1	No Dependencies	No Dependencies

Table 37 SAR Dependencies

6.3.2 Security Functional Requirements Rationale

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

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Authenticatio
FCS_CKM.1/AA													X
FCS_COP.1/AA													X
FIA_API.1/AA													X
FMT_MTD.1/AAK													X
FCS_CKM.1/CA Key pair		X											
FDP_ITC.1/PERSO KEY			X										
FDP_ITC.1/AA			X										X
FDP_ITC.1/CA		X	X										
FAU_SAS.1			X				X						

FCS_CKM.1/DH_PACE				X	X	X							
FCS_CKM.1/CA	X	X	X	X	X	X							
FCS_CKM.6	X		X	X	X	X							
FCS_COP.1/PACE_ENC						X							
FCS_COP.1/CA_ENC	X	X	X	X		X							
FCS_COP.1/PACE_MAC				X	X								
FCS_COP.1/CA_MAC	X	X	X	X									
FCS_COP.1/SIG_VER	X		X										
FCS_RNG.1	X		X	X	X	X							
FIA_AFL.1/PACE										X			
FIA_UID.1/PACE	X		X	X	X	X							
FIA_UAU.1/PACE	X		X	X	X	X							
FIA_UAU.4/PACE	X		X	X	X	X							
FIA_UAU.5/PACE	X		X	X	X	X							
FIA_UAU.6/PACE				X	X	X							
FIA_UAU.6/EAC	X		X	X	X	X							
FIA_API.1		X											
FDP_ACC.1/TRM	X		X	X		X							
FDP_ACF.1/TRM	X		X	X		X							
FDP_RIP.1				X	X	X							
FDP_UCT.1/TRM	X			X		X							
FDP_UTI.1/TRM				X		X							
FMT_SMF.1		X	X	X	X	X	X						
FMT_SMR.1/PACE		X	X	X	X	X	X						
FMT_LIM.1								X					
FMT_LIM.2								X					
FMT_MTD.1/INI_ENA			X				X						
FMT_MTD.1/INI_DIS			X				X						
FMT_MTD.1/CVCA_INI	X												
FMT_MTD.1/CVCA_UPD	X												
FMT_MTD.1/DATE	X												
FMT_MTD.1/CAPK	X	X		X									
FMT_MTD.1/PA			X	X	X	X							
FMT_MTD.1/KEY_READ	X	X	X	X	X	X							X
FMT_MTD.3	X												
FPT_EMS.1			X						X				
FPT_TST.1									X			X	
FPT_FLS.1									X			X	
FPT_PHP.3				X					X		X		
FPT_ITC.1/PACE				X	X	X				X			

Table 38 Security Objective Rationale

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

The security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document” addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1/KEY_READ and FMT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RNG.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RNG.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.6 after use.

In addition to the rationale above, the Personalization Agent imports the Active Authentication Private Key and Chip Authentication private according to **FDP_ITC.1/AA** and **FDP_ITC.1/CA** respectively. The Personalization Agent Key can be replaced by Personalization Agent after successfully authentication as required by **FDP_ITC.1/PERSO KEY**.

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FMT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and,

hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.6 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

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

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.6 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RNG.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.

This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).

FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.6 represent some required specific properties of the protocols used. The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key

FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.

The SFR FCS_RNG.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.

This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.6 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1/KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy.

The SFR FCS_RNG.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RNG.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.6 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA’s public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [5] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

In addition to the rationales above, the Chip Authentication Key is either loaded from outside the TOE as required by **FDP_ITC.1/CA** or generated by the TOE through **FCS_CKM.1/CA Key Pair**.

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

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

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

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).

This objective is achieved as follows:

- (i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
- (ii) for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) – FTP_ITC.1/PACE.

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

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

The security objective **OT.Active_Authentication** “Proof of MRTD’s chip authenticity through AA” is ensured by the Active Authentication Protocol provided by **FIA_API.1/AA** proving the authenticity of the chip. The

Active Authentication Protocol cryptographic operations covered by **FCS_COP.1/AA** are performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/AAK**, which is either loaded from outside the TOE as required by **FDP_ITC.1/AA** or generated by the TOE through **FCS_CKM.1/AA**. The SFR **FMT_MTD.1/KEY_READ** prevents read access to the secret key of the Active Authentication Private Keys

6.3.3 Security Assurance Requirements Rationale

The composite product package (COMP) was chosen to provide assurance that the TOE, being a composite product, has been assembled and evaluated in a way that conforms to the following objectives:

- ensure that the TOE has been composed of an already evaluated base component and a dependent component, considering the requirements given in CC Part 1 [CC:2022 P1] and CC Part 3 [CC:2022 P3];
- that the evaluation of STs, life cycle requirements, design, testing and vulnerability analysis for the composite product have been performed according to the criteria specified in CC Part 3 [CC:2022 P3].

The selection of the component ALC_FLR.1 provides assurance that the developer has established flaw remediation procedures that cover the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users

The rationales for the remaining Security Assurance Requirements are consistent with the ones described in the [PP0056] thus not presented here.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

This section is consistent with the one described in the [PP0056] thus not presented here.

6.3.5 Compatibility between SFRs of the TOE and [TMC_IC]

The table below lists the SFR defined by [TMC_IC] on which the SFR of this TOE is relying and they are separated in three groups:

- IP_SFR: Irrelevant base component-SFRs not being used by the Composite-ST.
- RP_SFR-SERV: Relevant base component-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
- RP_SFR-MECH: Relevant base component-SFRs being used by the Composite-ST because of their security properties providing protection against attacks to the TOE as a whole and being addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the base component.

● SFR of THD89	IP_SFR	RP_SFR-SERV	RP_SFR-MECH
FRU_FLT.2			FPT_PHP.3 FPT_FLS.1
FPT_FLS.1		FPT_FLS.1	
FMT_LIM.1		FMT_LIM.1	

FMT_LIM.2		FMT_LIM.2	
FAU_SAS.1		FAU_SAS.1	
FPT_PHP.3			FPT_PHP.3
FDP_ITT.1			FCS_CKM.1/CA Key pair FCS_CKM.1/AA FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_COP.1/AA FPT_EMS.1
FDP_IFC.1			FCS_CKM.1/CA Key pair FCS_CKM.1/AA FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_COP.1/AA FPT_EMS.1
FPT_ITT.1			FCS_CKM.1/CA Key pair FCS_CKM.1/AA FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_COP.1/AA FPT_EMS.1
FDP_SDC.1			FCS_CKM.1/CA Key pair FCS_CKM.1/AA FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC

			FCS_COP.1/SIG_VER FCS_COP.1/AA FPT_EMS.1
FDP_SDI.2			FPT_FLS.1 FPT_TST.1
FCS_RNG.1[PTG.2]		FCS_RNG.1	
FCS_COP.1[TDES]	X		
FCS_COP.1[RSA-CRT]		FCS_COP.1/AA FCS_COP.1/SIG_VE R	
FCS_COP.1[AES]		FCS_COP.1/PACE_E NC FCS_COP.1/PACE_ MAC FCS_COP.1/CA_EN C FCS_COP.1/CA_MA C	

Table 39 Compatibility between SFRs and [TMC_IC]

7 TOE Summary Specification

7.1 TSFs provided by the TMCICAO Application

The TSFs provided by the TMCICAO Application are listed in the table below:

Security Function	Name	SFR fulfillment
SF.AC	Access Control	FDP_ACC.1/TRM
		FDP_ACF.1/TRM
		FAU_SAS.1
		FMT_MTD.1/INI_ENA
		FMT_MTD.1/INI_DIS
		FMT_MTD.1/CVCA_INI
		FMT_MTD.1/CVCA_UPD
		FMT_MTD.1/DATE
		FMT_MTD.1/CAPK
		FMT_MTD.1/KEY_READ
		FMT_MTD.1/PA
		FMT_MTD.1/AAK
		FDP_ITC.1/PERSO KEY
		FDP_ITC.1/AA
		FDP_ITC.1/CA
		FMT_SMF.1
		FMT_SMR.1/PACE
SF.PACE	Password Authenticated Connection Establishment	FIA_AFL.1/PACE
		FIA_UID.1/PACE
		FIA_UAU.1/PACE
		FIA_UAU.4/PACE
		FIA_UAU.5/PACE
SF.SM	Secure Messaging	FTP_ITC.1/PACE
		FDP_UCT.1/TRM
		FDP_UIT.1/TRM
		FCS_COP.1/PACE_ENC
		FCS_COP.1/PACE_MAC
		FCS_CKM.1/DH_PACE
		FIA_UAU.6/PACE
		FIA_UAU.6/EAC
		FCS_RNG.1
		FCS_CKM.6
		FDP_RIP.1
		FCS_COP.1/CA_ENC
		FCS_COP.1/CA_MAC
SF.CA	Chip Authentication	FIA_API.1

		FCS_CKM.1/CA
		FCS_CKM.1/CA Key pair
SF.TA	Terminal Authentication	FMT_MTD.3
		FCS_COP.1/SIG_VER
SF.AA	Active Authentication	FIA_API.1/AA
		FCS_COP.1/AA
		FCS_CKM.1/AA
SF.SCP	Smart Card Platform	FPT_EMS.1
		FPT_FLS.1
		FPT_TST.1
		FPT_PHP.3
		FMT_LIM.1
		FMT_LIM.2

Table 40 Security Functions provided by the TMCICAO Application

SF.AC Access Control

The SF.AC function provides data access control mechanism on the logical MRTD:

- Only the BIS-PACE successfully authenticated by PACE authentication as defined in [ICAO9303] is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, and only the terminal successfully authenticated as Extended Inspection System is allowed to read the data in EF.DG3 and EF.DG4 of the logical MRTD. The above data can only be read by terminal using secure messaging. Thus **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM** are satisfied.
- A write-only-once mechanism is provided to the Manufacturer to write the IC Identification Data and Pre-personalization Data into TOE by which **FAU_SAS.1** and **FMT_MTD.1/INI_ENA** are satisfied.
- Life-cycle management ensures that only authorized Personalization Agent has the ability to disable the read access for the IC Identification Data. Therefore **FMT_MTD.1/INI_DIS** is met.
- The ability to write the initial CVCA Public Key, initial CVCA Certificate and initial Current Date is restricted to authorized Personalization Agent. Thus **FMT_MTD.1/CVCA_INI** is met.
- The ability to update the CVCA Public Key and CVCA Certificate is restricted to authorized Country Verifying Certification Authority. Therefore **FMT_MTD.1/CVCA_UPD** is fulfilled.
- The ability to modify the Current date is restricted to authorized Country Verifying Certification Authority, Document Verifier and Domestic Extended Inspection System. Therefore **FMT_MTD.1/DATE** is fulfilled.
- Only authorized Personalization Agent has the ability to create and load the Chip Authentication private key into TOE. Thus **FMT_MTD.1/CAPK** is satisfied.
- It is not allowed to read the PACE passwords, Chip Authentication Private Key and Personalization Agent Key from TOE by any roles. Thus **FMT_MTD.1/KEY_READ** is fulfilled.
- Only authorized Personalization Agent has the ability to write the Document Security Object into TOE. Therefore **FMT_MTD.1/PA** is met.
- Only authorized Personalization Agent has the ability to create and load the Active Authentication private key into TOE. Thus **FMT_MTD.1/AAK** is fulfilled.
- The Personalization Agent key can be replaced, Active Authentication keys and Chip Authentication keys can be loading when Personalization Agent successfully authenticate itself by presenting the previous version of the Personalization Agent Key. Thus **FDP_ITC.1/PERSO KEY**, **FDP_ITC.1/AA** and

FDP_ITC.1/CA are met.

- The life-cycle management maintains the following roles: Manufacturer, Personalization Agent, Terminal, PACE authenticated BIS-PACE, Country Verifying Certification Authority, Document Verifier, Domestic Extended Inspection System and Foreign Extended Inspection System in different life-cycle phases including Initialization, Pre-personalization, Personalization and Configuration. Thus **FMT_SMF.1** and **FMT_SMR.1/PACE** are met.

SF.PACE Password Authenticated Connection Establishment

SF.PACE provides the multiple authentication functionalities:

- SF.PACE allows user to read the Initialization Data in phase 2 “Manufacturing” before the user is identified. SF.PACE provides the identification of user. Specifically, SF_PACE identifies the role of user as MRTD manufacturer in Phase2 “Manufacturing”, Personalization Agent in Phase3 “Personalization of the MRTD”, and BIS-PACE and EIS in Phase 4 “Operational use”. Thus **FIA_UID.1/PACE** is fulfilled.
- SF.PACE provides the multiple authentication of user. Specifically, SF.PACE authenticates the user as MRTD manufacturer in Phase2 “Manufacturing”, Personalization Agent in Phase3 “Personalization of the MRTD” with the SCP03 protocol as defined in [GP]. SF.PACE allows the inspection system to authenticate the chip by verifying the signature generated in the chip through Active Authentication Protocol during phase 4. Meanwhile, SF.PACE authenticates the user as BIS-PACE in Phase 4 “Operational use” with the PACE protocol as defined in [ICAO9303]. Lastly, SF.PACE authenticates the user as EIS in Phase4 “Operational use” with Chip Authentication protocol and Terminal Authentication as defined in [TR03110-1]. After the successful SCP03 authentication, a secure channel in Phase 2 and Phase3 (AES as defined in [GP]) is established to protect the subsequent communication. After the successful PACE or CA authentication, a secure messaging in Phase 4 is established to protect the subsequent communication. Thus **FIA_UAU.1/PACE**, **FIA_UAU.4/PACE** and **FIA_UAU.5/PACE** are fulfilled.
- SF.PACE provides a failure handling that the processing time of PACE authentication increases an exponential number when unsuccessful attempts meet the configurable limitation in Phase 4 “Operational use”. Thus **FIA_AFL.1/PACE** is fulfilled.

SF.SM Secure Messaging

SF.SM provides the Secure Messaging functionalities:

- SF.SM protects the integrity of user data transferred between TOE and trusted IT product through the MAC authentication mechanism (conform to [FIPS 197] and [NIST-800-38B]) of Secure Messaging as defined in [ICAO9303], which fulfills **FDP_UIT.1/TRM**,
- SF.SM protects the confidentiality of user data transferred between TOE and trusted IT product through the AES encryption and decryption (conform to [FIPS 197] and [NIST-800-38B]) of Secure Messaging as defined in [ICAO9303], which fulfills **FDP_UCT.1/TRM**,
- SF.SM implements PACE secure messaging as communication channel between TOE and another trusted IT product. Therefore **FTP_ITC.1/PACE** is met.
- SF.SM implements the DH and ECDH key agreement algorithm (conform to [TR03111] and [PKCS3]), and generates the PACE secure messaging session keys as defined in [ICAO9303]. The key type is AES and the key size is 192 and 256 bits. Thus **FCS_CKM.1/DH_PACE** is fulfilled.
- SF.SM implements the continuous verification of security messaging, which provides the re-authentication of PACE/CA. Thus, the **FIA_UAU.6/PACE** and **FIA_UAU.6/EAC** are fulfilled.

- SF.SM destroys the secure messaging session keys and sensitive data when the Secure Messaging is terminated as defined in [ICAO9303] and [GP]. The session keys and sensitive data are re-written with random numbers. Thus **FCS_CKM.6** and **FDP_RIP.1** are met.
- SF.SM provides the random number generation (with TRNG generator) cryptographic functionality. Thus **FCS_RNG.1** is fulfilled,
- SF.SM implements the cryptographic operations used for PACE and CA Secure Messaging as defined in [ICAO9303], which includes the AES encryption and decryption for SM (conform to [FIPS 197] and [NIST-800-38B]). Thus **FCS_COP.1/PACE_ENC**, **FCS_COP.1/PACE_MAC**, **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_MAC** are fulfilled.

SF.CA Chip Authentication

The SF.CA function provides the Chip Authentication mechanism:

- The Chip Authentication is implemented as defined in [TR03110-1]. Thus **FIA_API.1** is satisfied.
- SF.CA implements the DH and ECDH key agreement algorithm (conform to [PKCS3] and [TR03110-1]), and generates the CA secure messaging session keys as defined in [ICAO9303]. The key type is AES and the key size is 192 and 256 bits. Thus **FCS_CKM.1/CA** is fulfilled.
- SF.CA provides the Chip Authentication Key on board generation functionality. Therefore **FCS_CKM.1/CA Key Pair** is met.

SF.TA Terminal Authentication

The SF.TA function provides the Terminal Authentication mechanism:

- SF.TA implements the validity verification of the certificate chain. Thus **FMT_MTD.3** is met.
- SF.TA implements the cryptographic operations used for TA digital signature verification as defined in [ICAO9303], which includes the RSA-CRT and ECC signature verification (conform to PKCS1 and [ICAO9303]). Thus **FCS_COP.1/SIG_VER** is satisfied.

SF.AA Active Authentication

The SF.AA function provides the Active Authentication mechanism:

- The Active Authentication is implemented as defined in [ICAO9303]. Thus **FIA_API.1/AA** is satisfied.
- SF.AA implements the digital signature generation used for Active Authentication as defined in [ICAO9303], which include the RSA-CRT (conform to [ISO 9796-2]) and ECDSA (conform to [TR03111]). Thus **FCS_COP.1/AA** is met.
- The Active Authentication cryptographic key pair is generated on board, which meets the standard: [TR03111]. Thus **FCS_CKM.1/AA** is fulfilled.

SF.SCP Smart Card Platform

The SF.SCP function uses the functionality provided by the platform to protect the data on TOE:

- The secret data is protected through bus masking, random branch insertion and random OSC clock jitter mechanisms provided by the platform to prevent emission. Thus **FPT_EMS.1** is fulfilled.
- The secure state is preserved when the failures occur. Thus **FPT_FLS.1** is met.
- The platform implements the self-test mechanism to protect the data on TOE. The key data is checked before any operation. The integrity of the TSF data and TSF executable code are verified by the security

function Memory Redundancy provided by certified IC. Thus **FPT_TST.1** is met.

- The environment sensors provided by the IC are enabled and configured to resist physical manipulation and physical probing. Thus **FPT_PHP.3** is fulfilled.
- The platform has implemented the hardware fuse mechanism to prevent using the test functionality after TOE delivery. Thus **FMT_LIM.1** and **FMT_LIM.2** are met.

7.2 TSFs provided by the IC

The TMCICAO evaluation depends on the result of IC evaluation. The following table lists the Security Functions provided by IC, details please refer to [TMC_IC].

Security Function	Description
Malfunction	Prevents malfunction attacks.
Leakage	Provides logical protection against leakage.
Physical manipulation and probing	Provides physical protection against physical probing and manipulation.
Abuse of functionality and Identification	Prevents abuse of test functionality delivered as part of the TOE.
Random numbers	Provides a random number generator.
Cryptographic functionality	Provides algorithm support.

Table 41 Security Functions provided by the IC

8 Appendix

8.1 Glossary and Acronyms

Term	Definition
<i>Accurate Terminal Certificate</i>	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR03110-1].
<i>Advanced Inspection Procedure (with PACE)</i>	A specific order of authentication steps between a travel document and a terminal as required by [ICAO9303], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO _D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
<i>Agreement</i>	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
<i>Active Authentication</i>	Security mechanism defined in [ICAO9303] 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 Organization.
<i>Application note</i>	Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
<i>Audit records</i>	Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalization Data.
<i>Authenticity</i>	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization
<i>Basic Access Control (BAC)</i>	Security mechanism defined in [ICAO9303] 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 (see there).
<i>Basic Inspection System with PACE protocol (BIS-PACE)</i>	A technical system being used by an inspecting authority and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorized by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document
<i>Basic Inspection System (BIS)</i>	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.

<i>Biographic data (biodata).</i>	The personalized 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. [ICAO9303]
<i>Biometric reference data</i>	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.
<i>Card Access Number (CAN)</i>	Password derived from a short number printed on the front side of the data-page.
<i>Certificate chain</i>	A sequence defining hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
<i>Counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO9303]
<i>Country Signing CA Certificate (C_{CSCA})</i>	Certificate of the Country Signing Certification Authority Public Key (K _{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
<i>Country Signing Certification Authority (CSCA)</i>	An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO9303]. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR03110-1].
<i>Country Verifying Certification Authority (CVCA)</i>	An organization enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a CVCS as a subject; hence, it merely represents an organizational entity within this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR03110-1].

<i>Current date</i>	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
<i>CV Certificate</i>	Card Verifiable Certificate according to [TR03110-1].
<i>CVCA link Certificate</i>	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
<i>Document Basic Access Key Derivation Algorithm</i>	The [ICAO9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
<i>PACE passwords</i>	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO9303],
<i>Document Details Data</i>	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
<i>Document Security Object (SO_D)</i>	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}). [ICAO9303]
<i>Document Signer (DS)</i>	An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C _{DS}), see [TR03110-1] and [ICAO9303]. This role is usually delegated to a Personalization Agent.
<i>Document Verifier (DV)</i>	An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [TR03110-1]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity within this ST. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy)

<i>Eavesdropper</i>	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
<i>Enrolment</i>	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO9303]
<i>Travel document (electronic)</i>	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
<i>ePassport application</i>	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine-readable travel document (MRTD). See [TR03110-1].
<i>Extended Access Control</i>	Security mechanism identified in [ICAO9303] 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.
<i>Extended Inspection System (EIS)</i>	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 Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO9303]
<i>Global Interoperability</i>	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. [ICAO9303]
<i>IC Dedicated Software</i>	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.
<i>IC Dedicated Support Software</i>	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.
<i>IC Dedicated Test Software</i>	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.

<i>IC Embedded Software</i>	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.
<i>IC Identification Data</i>	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.
<i>Impostor</i>	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. [ICAO9303]
<i>Improperly documented person</i>	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. [ICAO9303]
<i>Initialization</i>	Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
<i>Initialization Data</i>	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).
<i>Inspection</i>	The act of a State examining an travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO9303]
<i>Inspection system (IS)</i>	A technical system 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.
<i>Integrated circuit (IC)</i>	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
<i>Integrity</i>	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 Organization
<i>Issuing Organization</i>	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO9303]
<i>Issuing State</i>	The Country issuing the travel document. [ICAO9303]
<i>Logical Data Structure (LDS)</i>	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO9303]. The capacity expansion technology used is the travel document's chip.
<i>Logical travel document</i>	Data of the travel document holder stored according to the Logical Data Structure [ICAO9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1. personal data of the travel document holder 2. the digital Machine-Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2),

	4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
<i>Machine readable travel document (MRTD)</i>	Official document issued by a State or Organization 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. [ICAO9303]
<i>Machine readable zone (MRZ)</i>	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. [ICAO9303] The MRZ-Password is a restricted-revealable secret that is derived from the machine-readable zone and may be used for PACE.
<i>Machine-verifiable biometrics feature</i>	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. [ICAO9303]
<i>Manufacturer</i>	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.
<i>Metadata of a CV Certificate</i>	Data within the certificate body (excepting Public Key) as described in [TR03110-1]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorization Template, - Certificate Effective Date, - Certificate Expiration Date.
<i>ePassport application</i>	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 [ICAO9303], • 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.
<i>Optional biometric reference data</i>	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.

<i>Passive authentication</i>	(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.
<i>Password Authenticated Connection Establishment (PACE)</i>	A communication establishment protocol defined in [ICAO9303],. 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.
<i>PACE Password</i>	A password needed for PACE authentication, e.g. CAN or MRZ.
<i>Personalization</i>	The process by which the Personalization 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).
<i>Personalization Agent</i>	An organization acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [TR03110-1], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO9303] (in the role of DS). Please note that the role ‘Personalization 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.
<i>Personalization Data</i>	A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the life-cycle phase card issuing.
<i>Personalization Agent Authentication Information</i>	TSF data used for authentication proof and verification of the Personalization Agent.

<i>Personalization Agent Key</i>	Cryptographic authentication key used (i) by the Personalization 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 Personalization Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
<i>Physical part of the travel document</i>	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
<i>Pre-Personalization</i>	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
<i>Pre-personalization Data</i>	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalized 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 Personalization Agent Key Pair.
<i>Pre-personalized travel document's chip</i>	travel document's chip equipped with a unique identifier.
<i>Receiving State</i>	The Country to which the traveler is applying for entry. [ICAO9303]
<i>Reference data</i>	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.
<i>RF-terminal</i>	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
<i>Secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO9303]
<i>Secure messaging in encrypted/combined mode</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816-4]
<i>Service Provider</i>	An official organization (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
<i>Skimming</i>	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.
<i>Standard Inspection Procedure</i>	A specific order of authentication steps between a travel document and a terminal as required by [ICAO9303], namely (i) PACE or BAC and (ii) Passive Authentication with SO _D . SIP can generally be used by BIS-PACE and BIS-BAC.
<i>Terminal</i>	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).
<i>Terminal Authorization</i>	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.
<i>Terminal Authorization Level</i>	Intersection of the Certificate Holder Authorizations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
<i>TOE tracing data</i>	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognizing the travel document.
<i>Travel document</i>	Official document issued by a state or organization 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 [ICAO9303] (there “Machine readable travel document”).
<i>Travel Document Holder</i>	The rightful holder of the travel document for whom the issuing State or Organization personalized the travel document.
<i>Travel document’s Chip</i>	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [ISO14443] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO9303], sec III.
<i>Travel document’s Chip Embedded Software</i>	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.
<i>Traveler</i>	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
<i>TSF data</i>	Data created by and for the TOE that might affect the operation of the TOE ([CC:2022 P1]).
<i>Unpersonalized travel document</i>	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
<i>User data</i>	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [TR03110-1] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE.

	CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF ([CC:2022 P1]). 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:2022 P2]).
<i>Verification</i>	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. [ICAO9303]
<i>Verification data</i>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

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

8.2 Literature

Common Criteria

- [CC:2022 P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2022-11-001, CC:2022, Revision 1, November 2022
- [CC:2022 P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2022-11-002, CC:2022, Revision 1, November 2022
- [CC:2022 P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2022-11-003, CC:2022, Revision 1, November 2022
- [CC:2022 P4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities; CCMB-2022-11-004, CC:2022, Revision 1, November 2022
- [CC:2022 P5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements; CCMB-2022-11-005, CC:2022, Revision 1, November 2022
- [CEM:2022] Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2022-11-006, CEM:2022, Revision 1, November 2022
- [CC:TP] Transition Policy to CC:2022 and CEM:2022; CCMC-2023-04-001, April 20th, 2023
- [CC:EI] Errata and Interpretation for CC:2022 (Release 1) and CEM: 2022 (Release 1), Version 1.2, October 15th, 2025

Protection Profiles

- [PP0055] Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control; BSI-CC-PP-0055, Version 1.10, 25th March 2009
- [PP0056] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, Version 1.3.2, 05th December 2012
- [PP0068] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22th July 2014

ICAO

- [ICAO9303] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021, International Civil Aviation Organization
- [SAC] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014

Cryptography

- [ISO 9796-2] ISO/IEC 9796-2:2010, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, Third edition, 2010
- [ISO 9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, Second edition, 2011
- [ISO 11770-3] ISO/IEC 11770-3: Information technology – Security techniques – Key Management – Part3: Mechanisms using asymmetric techniques, 2008
- [FIPS 46-3] Federal Information Processing Standards Publication 46-3, Data Encryption Standard (DES); Reaffirmed October 1999
- [FIPS 180-4] Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS); August 2015
- [FIPS 186-5] Federal Information Processing Standards Publication 186-5, Digital Signature Standard (DSS); February 2023
- [FIPS 197] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES); November 2001
- [SP800-186] NIST Special Publication NIST SP 800-186, Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters; February 2023
- [RFC8017] RSA Laboratories, PKCS#1 v2.2: RSA Cryptography Standard, November, 2016
- [PKCS3] RSA Laboratories, PKCS#3 v1.4: Diffie-Hellman key-agreement standard, November 1, 1993
- [TR03111] Technical Guideline BSI TR-03111, Elliptic Curve Cryptography; Version 2.10, 2018-06-01

[ACM] European Cybersecurity Certification Group Sub-group on Cryptography
Agreed Cryptographic Mechanisms, Version 2.0 April 2025

TMC

[TMC_IC] THD89 Secure Microcontroller version 1.0 Security Target, version
2.2 November 2024

[AGD_OPE] TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE
configuration Operational User Guidance v0.7

[AGD_PRE] TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE
configuration Preparative procedures v0.6

[AGD_PG] TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE
configuration Personalization Guidance v0.6

[AGD_PPG] TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE
configuration Pre-Personalization Guidance v0.6

Other

[TR03110-1] Technical Guideline TR-03110-1, Advanced Security Mechanisms for
Machine Readable Travel Documents and eIDAS Token, Part1 –
eMRTDs with BAC/PACEv2 and EACv1; Version 2.20, 26.February
2015

[ISO7816-2] ISO/IEC 7816-2:2007, Identification cards – Integrated circuit(s) card –
Part2: Cards with contacts – Dimensions and location of the contacts

[ISO7816-4] ISO/IEC 7816-4:2013, Identification cards - Integrated circuit(s) card -
Part4: Organization, security and commands for interchange

[ISO14443] ISO/IEC 14443 Identification cards – Contactless integrated circuit cards
– Proximity cards, 2008-11

[GPPF] GlobalPlatform Technology Card Specification – Privacy Framework,
Version 1.0.1, November 2019