TMCICAO v1.0 on TMCOS 4.0 0.5

in ICAO BAC configuration

Security Target Lite

Common Criteria EAL4+

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

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 ..... - 9 -
1.4 TOE Description ..... - 9 -
1.4.1 TOE Physical Scope ..... - 9 -
1.4.2 TOE Logical Scope ..... - 10 -
1.4.3 TOE Life Cycle ..... - 11 -
2 Conformance Claims ..... - 14 -
2.1 CC Conformance Claim ..... - 14 -
2.2 CC PP Claim ..... - 14 -
2.3 CC Package Claim ..... - 14 -
2.4 Conformance Rationale ..... - 14 -
2.4.1 Conformity of the TOE type ..... - 15 -
2.4.2 SPD Consistency ..... - 15 -
2.4.3 Security Objectives Consistency ..... - 16 -
2.4.4 Conformity of the SFRs ..... - 17 -
3 Security Problem Definition ..... - 19 -
3.1 Introduction ..... - 19 -
3.2 Assumptions ..... - 19 -
3.3 Threats ..... - 19 -
3.4 Organizational Security Policies ..... - 19 -
4 Security Objectives ..... - 20 -
4.1 Security Objectives for the TOE ..... - 20 -
4.2 Security Objectives for the Operational Environment ..... - 20 -
4.3 Security Objectives Rationale ..... - 20 -
4.3.1 Rationale between Objectives and SPD ..... - 20 -
4.3.2 Compatibility between Objectives of the TOE and [TMC_IC] ..... - 21 -
5 Extended Components Definition ..... - 23 -
5.1 Definition of the Family FAU_SAS ..... - 23 -
5.1.1 Family behavior ..... - 23 -
5.1.2 Component leveling and description ..... - 23 -
5.1.3 Management of FAU_SAS.1 ..... - 23 -
5.1.4 Audit of FAU_SAS.1 ..... - 23 -
5.1.5 FAU_SAS.1 Audit storage ..... - 23 -
6 Security Requirements ..... - 24 -
6.1 Security Functional Requirements ..... - 25 -
6.1.1 Class FCS Cryptographic Support ..... - 25 -
6.1.2 Class FIA Identification and Authentication ..... - 28 -
6.1.3 Class FMT Security Management ..... - 29 -
6.1.4 Class FDP User Data Protection ..... - 30 -
6.1.5 Class FPT Protection of the Security Functions ..... - 31 -
6.2 Security Assurance Requirements ..... - 32 -
6.3 Security Requirements Rationale ..... - 32 -
6.3.1 Dependency Rationale ..... - 32 -
6.3.2 Security Functional Requirements Rationale ..... - 37 -
6.3.3 Security Assurance Requirements Rationale ..... - 40 -
6.3.4 Security Requirements – Mutual Support and Internal Consistency ..... - 41 -
6.3.5 Compatibility between SFRs of the TOE and [TMC_IC] ..... - 41 -

7 TOE Summary Specification ..... - 43 -
7.1 TSFs provided by the TMCICAO Application ..... - 43 -
7.2 TSFs provided by the IC ..... - 45 -
8 Appendix ..... - 46 -
8.1 Glossary and Acronyms ..... - 46 -
8.2 Literature ..... - 50 -

List of figures

Figure 1 Physical scope diagram..... - 9 -
Figure 2 TOE Life Cycle diagram..... - 11 -
Figure 3 FAU_SAS: Component leveling..... - 23 -

List of tables

Table 1 Comprise of TOE ..... - 10 -
Table 2 Role of the TOE components in the logical scope ..... - 10 -
Table 3 Overview of the life cycle of Composite product ..... - 12 -
Table 4 TOE Deliverables ..... - 12 -
Table 5 Assets Consistency table ..... - 15 -
Table 6 Subjects Consistency table ..... - 16 -
Table 7 Assumptions Consistency table ..... - 16 -
Table 8 Threats Consistency table ..... - 16 -
Table 9 Organizational Security Policies Consistency table ..... - 16 -
Table 10 Security objectives for the TOE Consistency table ..... - 17 -
Table 11 Security objectives for the OE Consistency table ..... - 17 -
Table 12 SFR Consistency table ..... - 18 -
Table 13 Security Objective Rationale ..... - 21 -
Table 14 Objectives for the TOE and [TMC_IC] compatibility table ..... - 21 -
Table 15 Objectives for OE compatibility table ..... - 22 -
Table 16 Definition of security attributes ..... - 24 -
Table 17 SFR list ..... - 25 -
Table 18 FCS_CKM.1/AA explanation ..... - 25 -
Table 19 FCS_CKM.6.1 explanation ..... - 26 -
Table 20 FCS_CKM.6.2 explanation ..... - 26 -
Table 21 FCS_COP.1/AUTH explanation ..... - 27 -
Table 22 FCS_COP.1/AA explanation ..... - 27 -
Table 23 Overview on authentication SFR ..... - 28 -
Table 24 FIA_AFL.1.1 explanation ..... - 29 -
Table 25 FIA_AFL.1.2 explanation ..... - 29 -
Table 26 FPT_EMS.1.1 table ..... - 32 -
Table 27 SFR Dependencies ..... - 35 -
Table 28 Non-satisfied Dependencies ..... - 36 -
Table 29 SAR Dependencies ..... - 37 -
Table 30 Security Objective Rationale ..... - 40 -
Table 31 Compatibility between SFRs and [TMC_IC] ..... - 42 -
Table 32 Security Functions provided by the TMCICAO Application ..... - 43 -
Table 33 Security Functions provided by the IC ..... - 45 -

1 ST Introduction

1.1 ST Reference

Title:	TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Security Target Lite
Version:	v1.1
Author:	Tongxin Microelectronics Co., Ltd
Publication Date:	2026-4-17

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 ICAO BAC 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 Basic Access Control according to [ICAO9303].

1.3.1 TOE Type

The Target of Evaluation (TOE) is the dual interface integrated circuit chip of machine-readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and Active Authentication according to [ICAO9303]. 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 MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity.
The MRTD in the context of this Security Target contains:

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

The authentication of the traveler and data access are based on:

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

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

For this security target the MRTD is viewed as unit of

a. the physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:

1. the biographical data on the biographical data page of the passport book,
2. the printed data in the Machine-Readable Zone (MRZ) and
3. the printed portrait.

b. the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder:

1. the digital Machine-Readable Zone Data (digital MRZ data, EF.DG1),
2. the digitized portraits (EF.DG2),
3. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both1,
4. the other data according to LDS (EF.DG5 to EF.DG16) and
5. the Document security object.

Major security features:

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

This Security Target covers the security features provided by the MRTD's chip. The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The logical MRTD 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 MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the [ICAO9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This Security Target addresses the protection of the logical MRTD:
1) in integrity by write-only-once access control and by physical means,
2) in confidentiality by the Basic Access Control Mechanism,
3) Active Authentication is used to prove the authenticity of the chip.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system:
1) reads optically the MRTD,
2) authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO9303].

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 Extended Access Control (EAC) and Password Authenticated Connection Establishment (PACE). However, these features are 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 MRTD, 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:

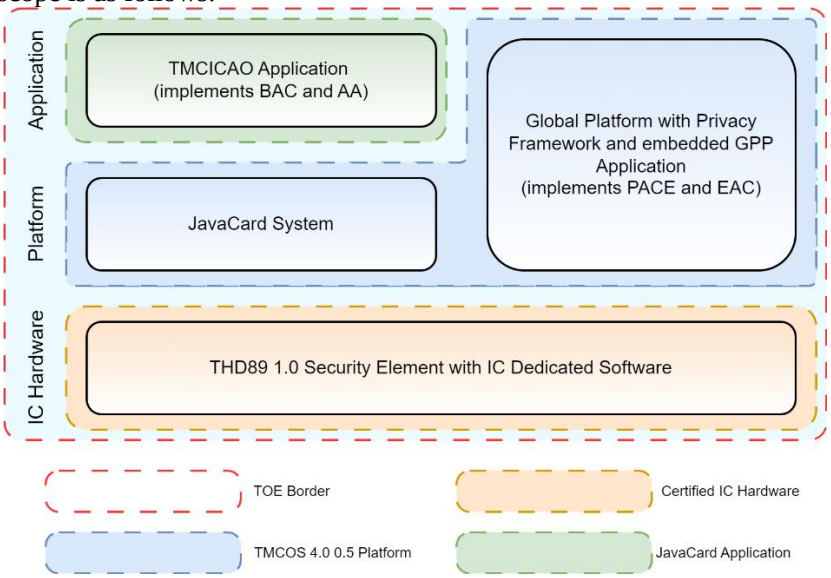

Figure 1 Physical scope diagram

This Security Target addresses the TOE in BAC 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 Basic Access Control Mechanism:

- Symmetric cryptography-based BAC authentication
- BAC Secure messaging
- Authorized read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16

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

- Active Authentication protocol as defined by [ICAO9303]

(3) 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.)

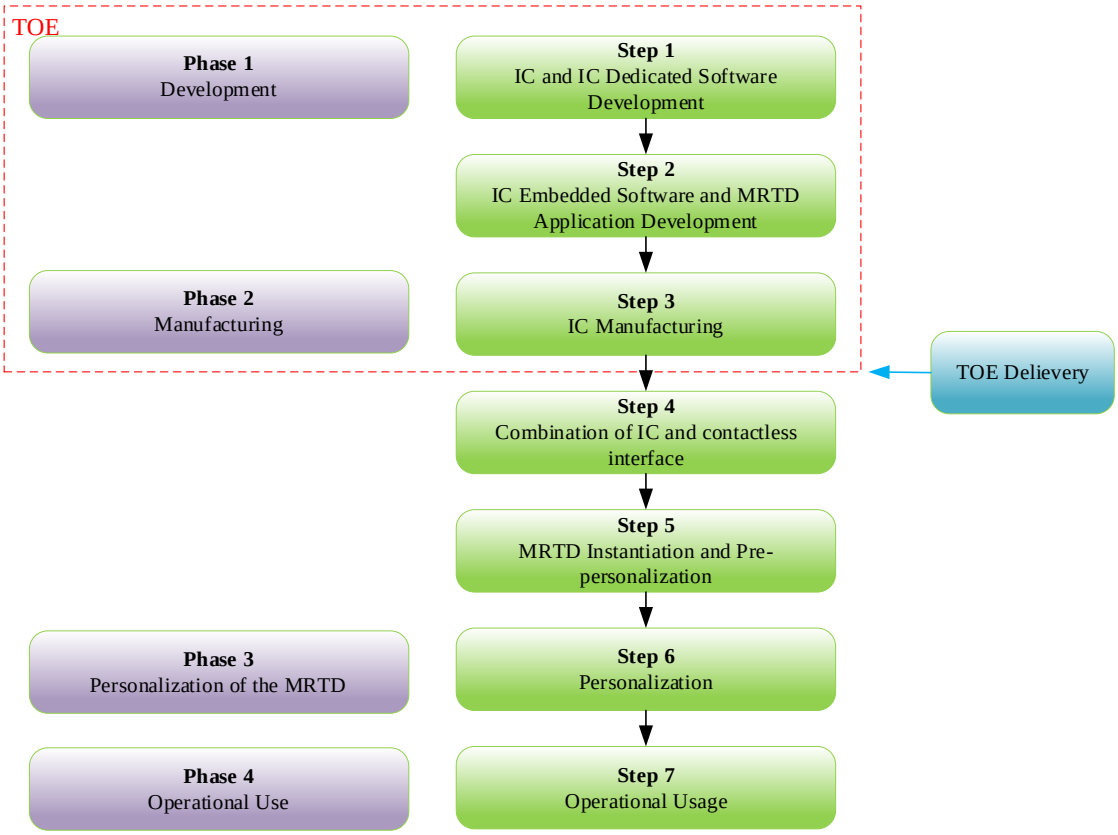

Figure 2 TOE Life Cycle diagram

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 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 MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step5) The MRTD manufacturer:

1) creates the MRTD application (i.e. the Applet instantiation) and

2) equips MRTD's chips with pre-personalization Data.

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

Phase 3 "Personalization of the MRTD"

(Step6) The personalization of the MRTD includes

a) the survey of the MRTD holder's biographical data,
b) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
c) the printing of the visual readable data onto the physical MRTD,
d) the writing of the TOE User Data and TSF Data into the logical MRTD and
e) configuration of the TSF if necessary.

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

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

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

Phase 4 "Operational Use"

(Step7) The TOE is used as MRTD 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 States 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 [PP0055]

2.3 CC Package Claim

The Security Target claims conformance to the assurance package EAL4 augmented with:

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

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 [PP0055] 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 [PP0055].
- Refinement (R): The element in the ST refines the corresponding [PP0055] 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 [PP0055] 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 [PP0055].

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.

The content of some "Application notes" present in [PP0055] may have been omitted or modified in this ST to avoid possible conflicts and inconsistencies of references / terminology / requirements used in [PP0055] 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 [PP0055]. 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 the dual interface (contactless and contact) integrated circuit chip of machine-readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and Active Authentication according to [ICAO9303], which is consistent with the TOE type defined in the [PP0055].

In addition to the contactless interface referred in the [PP0055], 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 [PP0055].

In addition to Basic Access Control, the TOE also implements Active Authentication. This is consistent with the TOE type in the [PP0055], as Active Authentication does not contradict or compromise the functionality provided by Basic Access Control. Moreover, the Active Authentication mechanism is defined in the same specification [ICAO9303], and its use can be considered complimentary to that of Basic Access Control

2.4.2 SPD Consistency

2.4.2.1 Assets consistency

All assets defined in [PP0055] are relevant for the TOE of this Security Target. The table below indicates the assets' consistency.

Assets	PP0055	Security Target
Logical MRTD Data	X	(E)
Authenticity of the MRTD's chip	X	(E)

Table 5 Assets Consistency table

2.4.2.2 Subjects consistency

All Subjects defined in [PP0055] are relevant for the TOE of this Security Target. The table below indicates the Subjects' consistency.

Subjects	PP0055	Security Target
Manufacturer	X	(E)
Personalization Agent	X	(E)
Terminal	X	(E)
Inspection system (IS)	X	(E)
MRTD Holder	X	(E)
Traveler	X	(E)
Attacker	X	(E)

Table 6 Subjects Consistency table

2.4.2.3 Assumptions consistency

All Assumptions defined in [PP0055] are relevant for the TOE of this Security Target. The table below indicates the Assumptions' consistency.

Assumptions	PP0055	Security Target
A.MRTD_Manufact	X	(E)
A.MRTD_Delivery	X	(E)
A.Pers_Agent	X	(E)
A.Insp_Sys	X	(E)
A.BAC-Keys	X	(E)

Table 7 Assumptions Consistency table

2.4.2.4 Threats consistency

All Threats defined in [PP0055] are relevant for the TOE of this Security Target. The table below indicates the Threats' consistency.

Threats	PP0055	Security Target
T.Chip_ID	X	(E)
T.Skimming	X	(E)
T.Eavesdropping	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.Counterfeit		(A)

Table 8 Threats Consistency table

2.4.2.5 Organizational Security Policies consistency

All OSPs defined in [PP0055] are relevant for the TOE of this Security Target. The table below indicates the OSPs' consistency.

OSPs	PP0055	Security Target
P.Manufact	X	(E)
P.Personalization	X	(E)
P.Personal_Data	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 [PP0055] are relevant for the TOE of this Security Target. The table below indicates the Security Objectives' consistency and the additions.

O.TOE	PP0055	Security Target
OT.AC_Pers	X	(E)

OT.Data_Int	X	(E)
OT.Data_Conf	X	(E)
OT.Identification	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.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 [PP0055] are relevant for the TOE of this Security Target. The table below indicates the Objective for Environment consistency and the additions.

O.ENV	PP0055	Security Target
OE.MRTD_Manufact	X	(E)
OE.MRTD_Delivery	X	(E)
OE.Personalization	X	(E)
OE.Pass_Auth-Sign	X	(E)
OE.BAC-Keys	X	(E)
OE.Exam_MRTD	X	(E)
OE.Passive_Auth-Verif	X	(E)
OE.Prot_Logical_MRTD	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 SFRs

2.4.4.1 SFR consistency

Several SFRs from [PP0055] have been adapted in this ST as BSI-CC-PP-0055 claims 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	PP0055	Security Target
FAU_SAS.1	X	(E)
FCS_CKM.1/AA		(A)
FCS_CKM.1	X	(E)
FCS_CKM.4	X	(M)
FCS_CKM.6		(M)
FCS_COP.1/SHA	X	(E)
FCS_COP.1/ENC	X	(E)
FCS_COP.1/AUTH	X	(E)
FCS_COP.1/MAC	X	(E)
FCS_COP.1/AA		(A)
FCS_RND.1	X	(M)
FCS_RNG.1		(M)
FIA_UID.1	X	(E)
FIA_UAU.1	X	(E)
FIA_UAU.4	X	(E)
FIA_UAU.5	X	(E)

FIA_UAU.6	X	(E)
FIA_AFL.1	X	(E)
FIA_API.1/AA		(A)
FDP_ACC.1	X	(E)
FDP_ACF.1	X	(R)
FDP_UCT.1	X	(E)
FDP_UIT.1	X	(E)
FDP_ITC.1/AA		(A)
FDP_ITC.1/PERSO KEY		(A)
FMT_SMF.1	X	(E)
FMT_SMR.1	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/KEY_WRITE	X	(E)
FMT_MTD.1/AAK		(A)
FMT_MTD.1/KEY_READ	X	(R)
FPT_EMSEC.1	X	(M)
FPT_EMS.1		(M)
FPT_FLS.1	X	(E)
FPT_TST.1	X	(E)
FPT_PHP.3	X	(E)

Table 12 SFR Consistency table

(1) The **FCS_CKM.4** is deprecated in the [CC:2022 P2], and replaced by **FCS_CKM.6**.
(2) The **FCS_RND.1** is in the Extended Components Definition part in the [PP0055], it is replaced by **FCS_RNG.1** in [CC:2022 P2].
(3) The **FDP_ACF.1** is refined to provide dependency for **FDP_ITC.1/PERSO KEY** and **FDP_ITC.1/AA**.
(4) The **FMT_MTD.1/KEY_READ** is refined to cover **OT.Active_Authentication**.
(5) The **FPT_EMSEC.1** is in the Extended Components Definition part in the [PP0055], it is replaced by **FPT_EMS.1** in [CC:2022 P2].
(6) The **FMT_LIM.1** and **FMT_LIM.2** are in the Extended Components Definition part in the [PP0055], they are included in [CC:2022 P2].
(7) 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**.
(8) 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 [PP0055] 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 [PP0055] 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 [PP0055] is not presented here. The complete list for the Threats is in the section 2.4.2.4. Added threat description is detailed below:

T.Counterfeit Counterfeit of MRTD chip data

An attacker with basic enhanced attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

3.4 Organizational Security Policies

The definition of OSPs from [PP0055] 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 [PP0055] are not repeated here. See section 2.4.3.1 for complete Security Objectives for the TOE.

Added Security Objectives for the TOE description are 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 enhanced basic attack potential.

4.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the Operational Environment from [PP0055] 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 [PP0055] is not presented here. Added rationales is detailed below:

	OT.Active_Authenticatio	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Counterfeit	X	X	X

Table 13 Security Objective Rationale

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.

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.AC_Pers		(C)
OT.Data_Int		(C)
OT.Data_Conf		(C)
OT.Identification	X	(I)
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.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 4 shows the component leveling for this family.

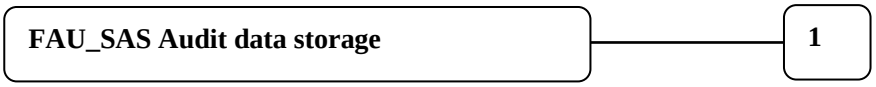

Figure 3 FAU_SAS: Component leveling

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.
FAU_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", "Basic Inspection System" 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 in section 8. The operations "write", "read", "modify", and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [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)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.
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 lists the SFRs that are copied directly from the [PP0055], all assignments and selections operations are taken as defined in the [PP0055]. These SFRs are not presented in this ST.

Security functional requirement	**Title**
FAU_SAS.1	Audit storage
FCS_CKM.1	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
FCS_COP.1/MAC	Cryptographic operation – Retail MAC
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication

FIA_UAU.6	Re-authenticating – Re-authenticating of Terminal by the TOE
FDP_ACC.1	Subset access control – Basic Access control
FDP_UCT.1	Basic data exchange confidentiality - MRTD
FDP_UIT.1	Data exchange integrity - MRTD
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre- personalization Data
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack

Table 17 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/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
ECC Key generation	***BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384 and NIST P-521***	***[TR03111] [SP800-186]***
RSA-CRT key generation	***2048, 3072 and 4096 bits***	***[RFC8017]***

Table 18 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.

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*** when ***following scenario*.**

Cryptographic keys	Scenario
BAC session keys	***(1) A Secure Messaging error occurs*** ***(2) A plain APDU is received***
Personalization session keys	***(1) The on-card Application Session is terminated.*** ***(2) The associated logical channel is explicitly closed.*** ***(3) The card is reset, deactivated or powered off: i.e. the Card Session ends***

Table 19 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
BAC session keys	***Clearing with random number***	***none***
Personalization session keys	***Clearing with random number***	***none***

Table 20 FCS_CKM.6.2 explanation

Application note: This Scenario in FCS_CKM.6.1 explanation is referenced from [ICAO9303] part 10 section 9.8.3 and [GP] section 10.2.3.

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

FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation

FCS_COP.1.1/SHA

The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic key sizes **none** that meet the following: ***FIPS 180-4.***

Application note: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive to derive the Basic Access Control Authentication Mechanism according to [ICAO9303]. The FIPS 180-2 as described in [PP0055] was superseded, the current revision is FIPS 180-4.

Application note: SHA-1 is supported by the product but not conformant with SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.3 [ACM]. However, as the TOE is a final ePassport TOE implementing BAC, the usage of such algorithm is mandated for the protocol implementation as defined by [ICAO9303]

FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES

FCS_COP.1.1/ENC

The TSF shall perform **secure messaging (BAC) – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bit** that meet the following: ***FIPS 46-3 and [ICAO9303], part11, section9.8 Secure Messaging*.**

Application note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH Cryptographic operation – Authentication

FCS_COP.1.1/AUTH

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

Algorithm	Key Size	Standard
Triple-DES	***112 bits***	***[FIPS 46-3]***
AES	***128 bits***	***[FIPS 197]***

Table 21 FCS_COP.1/AUTH explanation

Application note: The assignment of 112 bits Triple-DES in this SFR corresponds to the authentication of messages from the Terminal in a Basic Access Control secure channel. Triple-DES is supported by the product but not conformant with SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.3 [ACM]. However, as the TOE is a final ePassport TOE implementing BAC, the usage of such algorithm is mandated for the protocol implementation as defined by [ICAO9303]

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
RSA-CRT	***2048, 3072 and 4096 bits***	***[ISO 9796-2]***
ECDSA	***BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384 and NIST P-521***	***[TR03111] [SP800-186]***

Table 22 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 bits 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 used for the authentication protocols as required by FIA_UAU.4.

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	Algorithms and key sizes according to [ICAO9303]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bits keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bits keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES with 128 bits key (cf. FCS_COP.1/AUTH)
Active Authentication Protocol	FIA_API.1/AA	RSA-CRT, 2048, 3072 and 4096 bits ECDSA, 256, 384, 512 and 521 bits (cf. FCS_COP.1/AA)

Table 23 Overview on authentication SFR

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *AES*.

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.

Application note: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO9303]. In the first step the terminal authenticates itself to the MRTD’s chip and the MRTD’s chip authenticates to the terminal in the second step. In this second step the MRTD’s chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD’s chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1

The TSF shall provide
1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on ***AES*** to support user authentication.
FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the
1. the TOE accepts the authentication attempt as Personalization Agent by ***the Symmetric Authentication Mechanism with the Personalization Agent Key,***
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1

The TSF shall detect when ***following positive integer number*** unsuccessful authentication attempts occur related to ***following authentication events.***

Positive integer number	Authentication events
1	***Unsuccessful BAC authentication attempt***
32	***Unsuccessful SCP03 authentication attempt***

Table 24 FIA_AFL.1.1 explanation

FIA_AFL.1.2

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

Authentication events	Conditions	Actions
BAC	***met***	***Exponentially increasing time delay before new authentication attempt is possible***
SCP03	***surpassed***	***Exponentially increasing time delay before new authentication attempt is possible***

Table 25 FIA_AFL.1.2 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.

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

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

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 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/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 verb "load" means here that the Active 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 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 *Document Basic Access Keys, Personalization Agent Keys and Active Authentication Private Key* to **none.**

6.1.4 Class FDP User Data Protection

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

FDP_ACF.1 Basic Security attribute-based access control – Basic Access Control

FDP_ACF.1.1

The TSF shall enforce the **Basic Access Control SFP** to objects based on the following:
1. Subjects:
a. Personalization Agent,
b. Basic Inspection System,
c. Terminal,
2. Objects:
a. data EF.DG1 to EF.DG16 of the logical MRTD,
b. data in EF.COM,
c. data in EF.SOD,
d. all TOE intrinsic secret cryptographic keys stored in the travel document
3. Security attributes
a. authentication status of terminals.
FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.
FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the rule:
1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.
4. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1.

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 ***Basic 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/AA Import of user data without security attributes – Active Authentication Key

FDP_ITC.1.1

The TSF shall enforce the ***Basic 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.***

6.1.5 Class FPT Protection of the Security Functions

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

The TOE shall meet the requirement "TOE Emanation (FPT_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 following table:

ID	Emissions	Attack surface	TSF data	User data
1	***Electromagnetic emissions***	***Any***	***1. Personalization Agent Key*** ***2. Document Basic Access Keys*** ***3. Active Authentication Private Key***	***EF.DG1*** ***EF.DG2*** ***EF.DG5-DG16*** ***EF.SOD*** ***EF.COM***
2	***Current emissions***	***Smart card circuit contacts***		

Table 26 FPT_EMS.1.1 table

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 4 (EAL4) as defined in [CC:2022 P5], and the Composite Product Package (COMP) as defined in [CC:2022 P5].
And augmented by taking the following components:

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

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/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 [**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/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_CKM.1	[**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** 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**
FCS_COP.1/SHA	[**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	Justification 3 for non-satisfied dependencies **FDP_ITC.1** and **FCS_CKM.1**, see section 6.3.1.2 Justification 1 for non-satisfied dependencies **FCS_CKM.3**, see section 6.3.1.2
FCS_COP.1/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** Justification 1 for non-satisfied dependencies **FCS_CKM.3**, see section 6.3.1.2

FCS_COP.1/AUTH	[**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 **FDP_ITC.1/PERSO KEY** Justification 1 for non-satisfied dependencies **FCS_CKM.3**, see section 6.3.1.2
FCS_COP.1/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** Justification 1 for non-satisfied dependencies **FCS_CKM.3**, see section 6.3.1.2
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_UID.1	No dependencies	N/A
FIA_UAU.1	**FIA_UID.1** Timing of identification	Fulfilled by **FIA_UID.1**
FIA_UAU.4	No dependencies	N/A
FIA_UAU.5	No dependencies	N/A
FIA_UAU.6	No dependencies	N/A
FIA_AFL.1	**FIA_UAU.1** Timing of authentication	Fulfilled by **FIA_UAU.1**
FIA_API.1/AA	No dependencies	N/A
FDP_ACC.1	**FDP_ACF.1** Security attribute-based access control	Fulfilled by **FDP_ACF.1**
FDP_ACF.1	**FDP_ACC.1** Subset access control **FMT_MSA.3** Static attribute	Fulfilled by **FDP_ACC.1** Justification 4 for non-satisfied dependencies **FMT_MSA.3**, see section 6.3.1.2
FDP_UCT.1	[**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]	Justification 5 for non-satisfied dependencies **FTP_ITC.1** and **FTP_TRP.1**, see section 6.3.1.2 Fulfilled by **FDP_ACC.1**

FDP_UIT.1	[**FDP_ACC.1** Subset access control, or **FDP_IFC.1** Subset information flow control] [**FTP_ITC.1** Inter-TSF trusted channel, or **FTP_TRP.1** Trusted path]	Fulfilled by **FDP_ACC.1** Justification 5 for non-satisfied dependencies **FTP_ITC.1** and **FTP_TRP.1**, see section 6.3.1.2
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** Justification 6 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** Justification 6 for non-satisfied dependencies **FMT_MSA.3**, see section 6.3.1.2
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	**FIA_UID.1** Timing of identification	Fulfilled by **FIA_UID.1**
FMT_LIM.1	**FMT_LIM.2** 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** 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** Fulfilled by **FMT_SMF.1**
FMT_MTD.1/KEY_WRITE	**FMT_SMR.1** Security roles **FMT_SMF.1** Specification of Management Functions	Fulfilled by **FMT_SMR.1** 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** 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** Fulfilled by **FMT_SMF.1**
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 27 SFR Dependencies

6.3.1.2 Justification for non-satisfied dependencies

No.	SFR	Justification for non-satisfied dependencies
1	FCS_CKM.1/AA, FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, 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/AA	The SFR **FCS_CKM.1/AA** uses the asymmetric Active Authentication key generated or imported during the Personalization process (cf. **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	FCS_COP.1/SHA	The hash algorithm required by the SFR **FCS_COP.1/SHA** does not need any key material. Therefore, neither a key generation (**FCS_CKM.1**) nor an import (**FDP_ITC.1/2**) is necessary.
4	FDP_ACF.1	The access control TSF according to **FDP_ACF.1** uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR **FMT_MSA.1** and **FMT_MSA.3**) is necessary here.
5	FDP_UCT.1, FDP_UIT.1	The SFR **FDP_UCT.1** and **FDP_UIT.1** require the use secure messaging between the MRTD and the BIS. There is no need for SFR **FTP_ITC.1**, e.g. to require this communication channel to be logically distinct from other communication channel since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by **FTP_TRP.1** is not applicable here.
6	FDP_ITC.1/PERSO KEY, FDP_ITC.1/AA	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 both **FDP_ITC.1/PERSO KEY** and **FDP_ITC.1/AA**, the imported user data (the Personalization Key and the Active 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 28 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.3	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 29 SAR Dependencies

6.3.2 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Authenticatio
FAU_SAS.1				X					
FCS_CKM.1	X	X	X						
FCS_CKM.1/AA									X
FCS_CKM.6	X		X						
FCS_COP.1/SHA	X	X	X						
FCS_COP.1/ENC	X	X	X						
FCS_COP.1/AUTH	X	X							
FCS_COP.1/MAC	X	X	X						
FCS_COP.1/AA									X
FCS_RNG.1	X	X	X						
FIA_UID.1			X	X					
FIA_AFL.1			X	X					
FIA_UAU.1			X	X					
FIA_UAU.4	X	X	X						
FIA_UAU.5	X	X	X						
FIA_UAU.6	X	X	X						

FIA_API.1/AA									X
FDP_ACC.1	X	X	X						
FDP_ACF.1	X	X	X						
FDP_UCT.1	X	X	X						
FDP_UIT.1	X	X	X						
FDP_ITC.1/AA	X								X
FDP_ITC.1/PERSO KEY	X								
FMT_SMF.1	X	X	X						
FMT_SMR.1	X	X	X						
FMT_LIM.1								X	
FMT_LIM.2								X	
FMT_MTD.1/INI_ENA				X					
FMT_MTD.1/INI_DIS				X					
FMT_MTD.1/KEY_WRITE	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X						X
FMT_MTD.1/AAK									X
FPT_EMS.1	X				X				
FPT_TST.1					X		X		
FPT_FLS.1	X				X		X		
FPT_PHP.3	X				X	X			

Table 30 Coverage of Security Objective for the TOE by SFR

The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The Personalization Agent imports the Active Authentication Private Key according to FDP_ITC.1/AA. The Personalization Agent Key can be replaced by Personalization Agent after successfully authentication as required by FDP_ITC.1/PERSO KEY.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RNG.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [PP0056] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).

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

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.6, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4,

FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

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

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

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

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

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

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

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

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to

protect confidential TSF data stored and/or processed in the MRTD'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.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 EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The 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_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

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 selection of the component ADV_FSP.5 provides a higher assurance of the functional specification with semi-formal style and additional error messages with rationales.

The selection of the component ADV_INT.2 provides additional information to illustrate the entire TSF with

the well-structured internals.

The selection of the component ADV_TDS.4 provides higher assurance of the semiformal modular design and differentiating the SFR roles of the modules.

The selection of the component ALC_CMS.5 provides higher assurance of the configuration management with the additional development tools and related information.

The selection of the component ALC_TAT.2 provides higher assurance of the tools and techniques with the implementation standards applied by the developer.

The selection of the component ATE_DPT.3 provides higher assurance of the testing depth with all TSF modules tested.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

This section is consistent with the one described in the [PP0055] 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 FCS_CKM.1/AA FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/MAC FCS_COP.1/AUTH FCS_COP.1/AA FPT_EMS.1
FDP_IFC.1			FCS_CKM.1 FCS_CKM.1/AA FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/MAC FCS_COP.1/AUTH FCS_COP.1/AA FPT_EMS.1

FPT_ITT.1			FCS_CKM.1 FCS_CKM.1/AA FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/MAC FCS_COP.1/AUTH FCS_COP.1/AA FPT_EMS.1
FDP_SDC.1			FCS_CKM.1 FCS_CKM.1/AA FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/MAC FCS_COP.1/AUTH FCS_COP.1/AA FPT_EMS.1
FDP_SDI.2			FPT_FLS.1
FCS_RNG.1[PTG.2]		FCS_RNG.1	
FCS_COP.1[TDES]		FCS_COP.1/ENC FCS_COP.1/AUTH	
FCS_COP.1[RSA-CRT]		FCS_COP.1/AA	
FCS_COP.1[AES]		FCS_COP.1/AUTH	
FCS_COP.1[ECC]		FCS_COP.1/AA FCS_CKM.1/AA	

Table 31 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
		FDP_ACF.1
		FAU_SAS.1
		FMT_MTD.1/INI_ENA
		FMT_MTD.1/INI_DIS
		FMT_MTD.1/KEY_WRITE
		FMT_MTD.1/KEY_READ
		FMT_MTD.1/AAK
		FDP_ITC.1/AA
		FDP_ITC.1/PERSO KEY
		FMT_SMF.1
		FMT_SMR.1
SF.SYM_AUTH	Symmetric Authentication	FIA_AFL.1
		FIA_UID.1
		FIA_UAU.1
		FIA_UAU.4
		FIA_UAU.5
SF.SM	Secure Messaging	FDP_UCT.1
		FDP_UIT.1
		FCS_CKM.1
		FCS_CKM.6
		FCS_COP.1/SHA
		FCS_COP.1/ENC
		FCS_COP.1/AUTH
		FCS_COP.1/MAC
		FIA_UAU.6
		FCS_RNG.1
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 32 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 Personalization Agent successfully authenticated by SCP03 as defined in [GP] is allowed to write the data of EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, and only the Basic Inspection System successfully authenticated by Basic Access Control 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. Thus **FDP_ACC.1** and **FDP_ACF.1** 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 Document Basic Access Key into TOE is restricted to authorized Personalization Agent. This is to meet **FMT_MTD.1/KEY_WRITE**.
- It is not allowed to read the Active Authentication Private Keys, Document Basic Access 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 create and load the Active Authentication private key into TOE. Thus **FMT_MTD.1/AAK** is fulfilled.
- The Personalization Agent key can be replaced, and Active 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** and **FDP_ITC.1/AA** are met.
- The life-cycle management maintains the following roles: Manufacturer, Personalization Agent and Basic Inspection System in different life-cycle phases including Initialization, Pre-personalization and Personalization. Thus **FMT_SMF.1** and **FMT_SMR.1** are met.

SF.SYM_AUTH Symmetric authentication

SF.SYM_AUTH provides the symmetric authentication functionalities:
- SF.SYM_AUTH allows user to read the Initialization Data in phase 2 “Manufacturing”, read the random identifier in Phase3 “Personalization of the MRTD” and Phase 4 “Operational Use” before the user is identified. SF.SYM_AUTH provides the identification of user. Specifically, SF.SYM_AUTH identifies the role of user as MRTD manufacturer in Phase2 “Manufacturing”, Personalization Agent in Phase3 “Personalization of the MRTD”, and Basic Inspection System in Phase 4 “Operational use”. Thus **FIA_UID.1** is fulfilled.
- SF.SYM_AUTH provides the symmetric authentication of user. Specifically, SF.SYM_AUTH 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.SYM_AUTH also authenticates the user as Basic Inspection System in Phase 4 “Operational use” with the BAC protocol as defined in [ICAO9303]. After the successful authentication, a SCP03 secure channel in Phase 2 and Phase3 (AES as defined in [GP]), or a secure messaging in Phase 4 (3DES as defined in [ICAO9303]) is established to protect the subsequent communication. Thus **FIA_UAU.1**, **FIA_UAU.4** and **FIA_UAU.5** are fulfilled.
- SF.SYM_AUTH provides a failure handling that the processing time of BAC authentication and SCP03 authentication increases an exponential number when unsuccessful attempts meet the configurable limitation. Thus **FIA_AFL.1** 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 46-3] and [ISO 9797-1]) of Secure Messaging as defined in [ICAO9303], which fulfills **FDP_UIT.1**,
- SF.SM protects the confidentiality of user data transferred between TOE and trusted IT product through the 3DES encryption and decryption (conform to [FIPS 46-3] and [ISO 9797-1]) of Secure Messaging as defined in [ICAO9303], which fulfills **FDP_UCT.1**,
- SF.SM generates the secure messaging session keys through the BAC mechanism as defined in [ICAO9303]. The key type is 3DES and the key size is 112 bits [FIPS 46-3]. Thus **FCS_CKM.1** is fulfilled,
- SF.SM destroys the secure messaging session keys when the Secure Messaging is terminated as defined in [ICAO9303] and [GP]. The session keys are re-written with random numbers, as defined in **FCS_CKM.6**,
- SF.SM implements the cryptographic operations used for BAC authentication defined in [ICAO9303], which include the random number generation (with TRNG generator), the SHA1 message digest calculation (conform to [FIPS 180-4]) for Document Basic Access Key derivation, and the 3DES encryption and decryption during BAC authentication (conform to [FIPS 46-3] and [ISO 9797-1]). Thus **FCS_RNG.1**, **FCS_COP.1/SHA** and **FCS_COP.1/AUTH** are fulfilled,
- SF.SM implements the cryptographic operations used for Secure Messaging as defined in [ICAO9303],

which include the 3DES encryption and decryption for SM (conform to [FIPS 46-3] and [ISO 9797-1]). Thus **FCS_COP.1/ENC** and **FCS_COP.1/MAC** are fulfilled.
- SF.SM implements the continuous verification of security messaging, which provides the re-authentication of BAC. Thus **FIA_UAU.6** is fulfilled.

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 and meet 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 33 Security Functions provided by the IC

8 Appendix

8.1 Glossary and Acronyms

Term	Definition
Active Authentication	Security mechanism defined in [ICAO9303] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State or Organization.
Application note	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.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control (BAC)	Security mechanism defined in [ICAO9303] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the MRTD holder of the document appearing as text in the visual and machine-readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO9303]
biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO9303]
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key (K_{PuCSCA}) issued by CSCA stored in the inspection system
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAO9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [ICAO9303]
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO9303]
Extended Access Control	Security mechanism identified in [ICAO9303] by which means the MRTD'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. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO9303]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine-readable data in all MRTDs. [ICAO9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO9303]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO9303]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. section 1.4.3, TOE Life Cycle, Phase 2, Step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO9303]
Issuing State	The Country issuing the MRTD. [ICAO9303]

Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO9303]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAO9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD 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
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	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]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO9303]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO9303]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO9303]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD'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.DG14, EF.DG 16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [ICAO FAL12], p. 14.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD'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 finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. section 1.4.3, TOE Life Cycle, Phase 3, Step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel document	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.
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. section 1.4.3, TOE Life Cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism
random identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.
Receiving State	The Country to which the Traveler is applying for entry. [ICAO9303]

reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO9303]
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Travel document	A passport or other official document of identity issued by a State or Organization, which may be used by the rightful holder for international travel. [ICAO9303]
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. [CC:2022 P1]
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF. [CC:2022 P1]
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO9303]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Term	Definition
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
MF	Master File
N/A	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functions

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 1.3.0, 20th January 2012

[PP0068] Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, (PACE PP); BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011

[PP0084] Security IC Platform Protection Profile with Augmentation Packages; BSI-CC-PP-0084-2014, Version 1.0, 13.01.2014

ICAO

[ICAO9303] ICAO Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021, International Civil Aviation Organization

[ICAO FAL12] ICAO Facilitation (FAL) Division, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

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 14443] ISO/IEC 14443:2016, Identification cards – Contactless integrated circuit(s) card – Proximity cards

[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 BAC configuration Operational User Guidance v0.7

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

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

[AGD_PPG] TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC 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
[GP]	GlobalPlatform Technology Card Specification; GPC_SPE_034, Version 2.3.1, March 2018
[JCRE]	Java Card Platform Runtime Environment Specification, Classic Edition; Version 3.1, February 2021
[JCVM]	Java Card Platform Virtual Machine Specification, Classic Edition; Version 3.1, February 2021
[JCAPI]	Java Card Platform, version 3.1 Application Programming Interface. February 2021.
[GPPF]	GlobalPlatform Technology Card Specification – Privacy Framework, Version 1.0.1, November 2019

