Security Target Lite
KCOS e-Passport Version 5.0
– BAC and AA on S3D350A Family

Date : 2019. 06. 10.

Filename : EPS-05-AN-ST-BAC(Lite)

KOMSCO
Technology Research Institute
IT Research Department

The certified ST is written in Korean(including some English). This document is a translation of the original from Korean into English.

This page left blank on purpose for double-side printing.

KOMSCO Korea Minting, Security Printing & ID Card Operating Corp.	Revision History	Document	EPS-05-AN-ST-BAC(Lite)

개정번호	변경 내용	변경일	비고
1.0	New Publication	2019.06.10	

<Table of Contents>

<List of Tables>

<List of Figures>

1. ST Introduction

1.1. ST Reference

Title	Security Target <EPS-05-AN-ST-BAC(Lite)>
Date	2019.06.10
Assurance Level	EAL4+ (ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3)
Protection Profile	BSI-PP-0055, version 1.10, 25th March 2009 [BACPassPP]
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Editor(s)	KOMSCO
Keywords	MRTD, e-Passport, BAC, AA

1.2. TOE Reference

TOE name	· KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family - K5.0.01.SS.D35A.02(S3D350A) - K5.0.01.SS.D30A.02(S3D300A) - K5.0.01.SS.D26A.02(S3D264A) - K5.0.01.SS.D32A.02(S3D232A)
TOE version	Version 5.0
TOE developer	KOMSCO
TOE component	- IC chip : Samsung S3D350A Family[HWCR] (ANSSI-CC-2019/01) • including the IC Dedicated Crypto Library S/W - IC Embedded Software(OS) : KCOS e-Passport Version 5.0 - BAC and AA - The guidance documentation • EPS-05-QT-OPE-BAC-1.0 • EPS-05-QT-PRE-BAC-1.0

1 The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in Flash. These data are available by executing a dedicated command.

2 This identification data is described in the TOE guidance documentation. A more detailed explanation is described in the preparation guide(AGD-PRE)

1.3. TOE Overview

3 The TOE is the native chip operating system(COS), MRTD application and MRTD application data implemented on the IC chip and additionally includes S3D350A/300A/264A/232A version 2, which is a contactless IC chip of Samsung Electronics and is certified according to CC EAL 6+(ANSSI-CC-2019/01).

4 According to the Technical Guideline [EAC-TR] and [ICAO 9303], the ePassport Application supports Passive Authentication, Password Authenticated Connection Establishment (PACE), Terminal and Chip Authentication(EAC), Active Authentication(AA) and also Basic Access Control (BAC).

5 In this Security Target, only BAC and AA are considered for evaluation.

6 the TOE also carries out the PAC (Personalization Access Control), which is a security mechanism for the secure personalization and management on the personalization phase at the Personalization Agent.

7 The main objectives of this ST are:

- To introduce TOE and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

8 The TOE uses generation of random numbers. TDES, AES, Retail MAC, CMAC, RSA and ECC supported by the MRTD chip.

9 Since The TOE is a composite evaluation product, it includes IC chip, COS, application programs, and etc. There is no non-TOE HW/FW/SW requested to perform TOE security attributes. Note, the RF antenna and the booklet are needed to represent a complete MRTD to ePassport holder, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.4. TOE Definition

10 The Target of Evaluation (TOE) is the contactless 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 according to [ICAO-9303]

In addition to [BACPassPP], the TOE supports the active authentication as defined in [ICAO-9303].

The TOE comprises at least

- the circuitry of the travel document's chips(the integrated circuit, IC)
- the IC Dedicated Software and the IC Dedicated Support Software
- the IC Embedded Software(operating system),
- the epassport application compliant with [ICAO-9303]
- the associated guidance documentation

1.4.1. TOE usage and security features for operational

11 A State or Organization issues travel documents to be used by the holder for international travel. The traveller presents a travel document to the inspection system to prove his or her identity. The travel document in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the travel document's chip according to LDS in case of contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

For this security target the travel document is viewed as unit of

12 (i) **the physical part of the travel document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder

(a) the biographical data on the biographical data page of the travel document surface,

(b) the printed data in the Machine Readable Zone (MRZ) and

(c) the printed portrait.

13 (ii) **the logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO-9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal

data of the travel document holder

(a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(b) the digitized portraits (EF.DG2),

(c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both

(d) the other data according to LDS (EF.DG5 to EF.DG16) and

(e) the Document Security Object (SOD).

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

15 The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [ICAO-9303]. These security measures can include the binding of the travel document's chip to the passport book.

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

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

18 This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This security target addresses the Active Authentication but does not address the Extended Access Control.

19 The Basic Access Control is a security feature which is mandatory supported by the TOE.
The inspection system (i) reads optically the travel document, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the travel document' chip provides read access to the logical travel document by means of private communication (Secure Messaging) with this inspection system [ICAO-9303].

1.4.2. TOE Life Cycle

20 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP-IC-0084], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

21 Phase 1 “Development”

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software(COS), the ePassport application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

22 Phase 2 “Manufacturing”

(Step3) The TOE integrated circuit is produced by the IC manufacturer conforming with KOMSCO requirements. The IC manufacturer writes the IC Identification Data onto the chip to control the IC during the IC as travel document material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

If necessary, the IC manufacturer adds the parts of the IC embedded Software in the non-volatile programmable memories (FLASH)

(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step5) The MRTD manufacturer (i) Initializes the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.

The pre-personalized MRTD together with the IC Identifier are securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

23 Phase 3 “Personalization of the travel document”

(Step6) The personalization of the MRTD includes

(i) the survey of the MRTD holder’s biographical data,

(ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),

(iii) the printing of the visual readable data onto the physical part of the MRTD,

(iv) the writing of the TOE User Data and TSF Data into the logical MRTD and

(v) configuration of the TSF if necessary.

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

(i) the digital MRZ data (EF.DG1),

(ii) the digitized portrait (EF.DG2), and

(iii) the Document security object.

The signing of the Document security object by the Document signer 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.

24 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 State but they can never be modified.

25 **Application note 1 :** In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

Actors

(Table 1-1) Identification of the actors

Actors	Identification
Integrated Circuit (IC) Developer	Samsung
Embedded Software Developer	KOMSCO
Integrated Circuit (IC) Manufacturer	Samsung
Code Image Downloader	KOMSCO or Samsung
Pre-personalizer	KOMSCO or Samsung
MRTD manufacturer	KOMSCO or another printer
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

26 The TOE is a composite evaluation product. For this reason, the evaluation of from (Step 1) to (Step 3) coverd by ALC assurance. And then, the process of delivery between ePassport/Inlay manufacturer, Personalization agent and ePassport holder is not included in the scope of this evaluation.

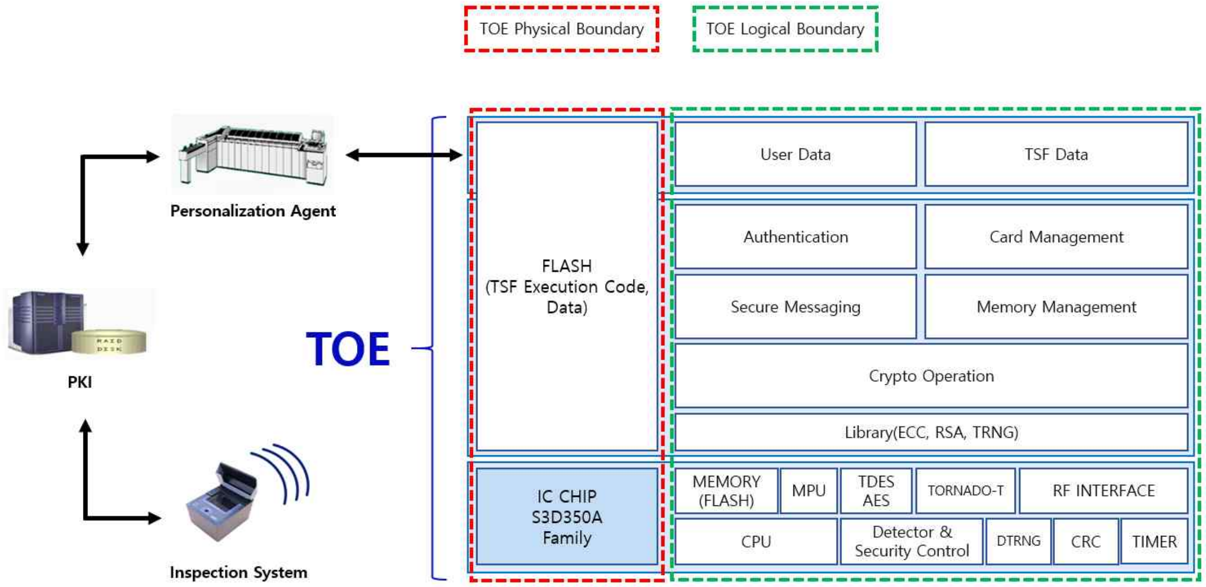
1.4.3. TOE Physical Boundaries

27 The physical TOE is the following:

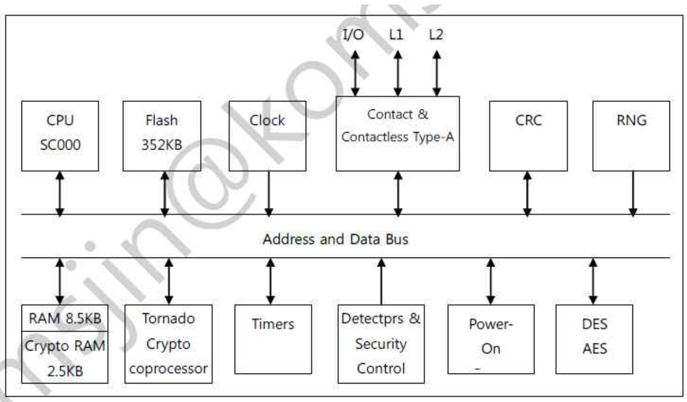
- the integrated circuit chip S3D350A Family(microcontoller) programmed with the operating system and with the ICAO application.

The components of chip are CPU, Crypto Co-Processor, I/O, Memory(RAM, FLASH), and various H/W functions.

In IC Chip’s flash area, after e-passport application is installed, flash area is changed locked state.(Lock NVM attribute). And also, e-passport data like biometric data (face, fingerprint) and TSF data(keys for authentication such as PAC private key, BAC key and AA private key) are saved in the flash area.



[Figure 1-1] TOE Physical/Logical Boundaries



Samsung S3D350A Family which is the composition element of he IC chip, is a product certified with CCRA EAL 6+ assurance level, and the composition elements included in the authentication are IC chip hardware and cryptogaphic calculation software library as shown in the following.

(Table 1-1) TOE Components Identification

Classification		Identification information	Delivery form/method
TOE	IC Chip + COS + Application	· KCOS e-Passport Version 5.0 - BAC and AA on S3D350A Family - K5.0.01.SS.D35A.02(S3D350A) - K5.0.01.SS.D30A.02(S3D300A) - K5.0.01.SS.D26A.02(S3D264A)	IC Chip (COB Format)/by a person

		- K5.0.01.SS.D23A.02(S3D232A)	
TOE Components	IC Chip (HW)	S3D350A/S3D300A/S3D264A/S3D232A revision 2	wafer or module/ by a person
	IC Dedicated SW	Secure Boot loader & System API Code v0.7 (07_S3D350A_Bootloader_SystemAPI_Release_v0_7_20170222.zip) DTRNG FRO library v2.0 (S3D350A_DTRNG_FRO_Library_v2.0_LETI_delivery_20171012.zip) AT1 Secure RSA/ECC/SHA Library v2.01 (20180802_PKA_lib_AT1_v2.01.zip)	Soft copy/PGP email
	COS+Application (SW)	KCOS e-Passport Version 5.0 – BAC and AA · FLASH image - KCOS50_350A.hex-1.3 - KCOS50_300A.hex-1.3 - KCOS50_264A.hex-1.3 - KCOS50_232A.hex-1.3 ⇒ included certified crypto library of IC chip	FLASH code/ PGP email
	DOC	- AGD_OPE : EPS-05-QT-OPE-BAC-1.0 - AGD_PRE : EPS-05-QT-PRE-BAC-1.0	Soft copy or Book/ PGP email or a person

1.4.4. TOE Logical Boundaries

28 KCOS e-Passport Version 5.0 – BAC and AA operating system manages all the resources of the integrated circuit that equips the passport, providing secure access to data and functions. Major tasks performed by operating system are:

- Communication with external devices(Inspection System and Personalization Agent)
- Data storage in the file system and secure memory area
- Dispatch and execution of commands
- Cryptographic operation
- Management of the security policies

Logical area in Figure 1-1 shows an overview of the TOE architecture.

- Crypto Operation : provides the cryptographic services(Triple-DES, AES, SHA, MAC, RSA, ECC etc.)
- Authentication : loading of keys related to authentication and the function of authentication such as PAC, BAC, AA
- Card Management : sending and receiving of APDU, integrity checking, clearing of residual information and the function for preservation of TOE secure state
- Memory Management : creating, selection, deleting of files and management of transaction
- Secure Messaging : securemessaging for secure communication channel
- User Data : All data(being not authentication data) stored in the context of the ePassport application of travel document as defined in [EAC-TR] and [ICAO-9303] such as EF.DG1, EF.DG2, EF.DG5 ~ EF.DG16
- TSF Data : Data created by and for the TOE that might affect the operation of the TOE including the private authentication key such as PAC private key, BAC key and AA private key

Security Mechanism

29 The TOE provides security features such as confidentiality, integrity, access control and authentication for e-Passport personalization data and TSF data security. These security features implemented as BAC security mechanism which defined [ICAO-9303] and PAC security mechanism for personalization. Also, The TOE consists of PA authentication for detect e-Passport personalization data forgery through digital signature verification of SOD which is from TOE to verification system and AA authentication features.

< PAC(Personalization Access Control) >

30 The TOE provides the PAC security mechanism which consists of PAC mutual authentication and PAC session key generation used for access control of Personalization Agent in initialization phase and personalization phase.

The PAC authentication is entity authentication protocol based on TDES/AES to authenticate between Personalization Agent and TOE in personalization phase. The PAC authentication uses TDES/AES algorithm.

The PAC session key generation feature is to make PAC session key(i.e. PAC session crypto key and PAC session MAC key) in order to create secure channel between TOE and Personalization Agent. The PAC session key generation is implemented by key derivation protocol based on TDES/AES. The way to create secure channel is similar to that of the BAC mechanism.

< BAC(Basic Access Control) >

31 Basic Access Control provides mutual authentication and session key establishment by means of a three-step challenge-response protocol, Key Establishment Mechanism using Triple DES [FIPS PUB 46-3] as block cipher. A cryptographic checksum according to [ISO_9797-1], MAC Algorithm 3, is calculated over and appended to the ciphertexts. The modes of operation described in [ICAO-9303] are used. Exchanged nonces must be 8 bytes long, exchanged keying material must be 16 bytes long.

< PA(Passive Authentication) >

32 The integrity of data stored under the LDS is checked by means of the Passive Authentication mechanism defined in [ICAO-9303]. Passive Authentication consists of the following steps :

1. The inspection system reads the Document Security Object (SOD), which contains the Document Signer Certificate from the IC.
2. The inspection system builds and validates a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SOD).
3. The inspection system uses the verified Document Signer Public Key to verify the signature of the Document Security Object (SOD).
4. The inspection system reads relevant data groups from the IC.
5. The inspection system ensures that the contents of the data groups are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SOD).

< AA(Active Authentication) >

33 Active Authentication authenticates the IC by signing a challenge sent by the inspection system with a private key known only to the IC[ICAO-9303].

For this purpose, the IC 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 is therefore authenticated by the issuer's digital signature. The corresponding private key is stored in the IC secure memory.

By authenticating the Document Security Object (SOD) and Data Group 15 by means of Passive Authentication in combination with Active Authentication, the inspection system verifies that the

Document Security Object (SOD) has been read from a genuine IC.

Additional Security Features

34 The TOE provides crypto operation, identification, authentication and access control through the PAC and BAC secure mechanism.

The TOE manages the function such as Initialization, Pre-personalisation, Personalisation and managing TSF data such as crypto key for security mechanism and certifications. Also, The TOE manages the security role such as Manufacturer, Personalisation Agent, Terminal.

The TOE performs self test and provides integrity check way to ensure secure operation. While in operation, The TOE operates countermeasure from DPA/SPA technique which is extracting crypto information by analysing the physical phenomenon(such as current, voltage, electro-magnetic). Also, it provides protection countermeasure from physical invasion.

IC Chip Providing Features

35 IC chip is composed of a processing unit, security components, contactless and contact based I/O ports. IC chip also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including optional public key cryptographic libraries, a random number generation library and an random number generator. The public key cryptographic libraries further include the functionality of hash computation.

IC chip also supports the feature :

security Security sensors, detectors or filters

- Shields
- Life time detector
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks

(Table 1-2) The main feature of IC chip and usage in TOE

The feature of IC chip		usage in TOE
Security	• TDES	○
	• AES	○
	• RSA • ECC	○
	• SHA-2	○
	• RNG	○(DTRNG)
	• Abnormal condition detectors	○
	• MPU	○
	• MEMORY ENCRYPTION	○
	• Random Branch Insertion(RBI)	○
	• Variable Clock	○
Communication	• ISO7816 contact interface	X
	• ISO14443 contactless interface	○

2. Conformance Claims (ASE_CCL.1)

2.1. CC Conformance Claim

36 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

- Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,
- Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,
- Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

as follows:

- Part 2 extended,
- Part 3 conformant.

37 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 ([CC]) has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

2.2. PP Claim

38 This ST claims strict conformance to ‘Common Criteria Protection Profile Machine Read-able Travel Document with ICAO Application” Basic Access Control’, Version 1.10, BSI-CC-PP-0055 issued by Bundesamt für Sicherheit in der Informationstechnik (BSI) [BACPassPP].

39 **Application note 2** : The IC chip, which is a component of the TOE, complies with the Security IC Platform Protection Profile with Augmentation Packages, Version 1.0 (BSI-CC-PP-0084-2014). Refer to ST[HWST] of the IC chip for rationale of conformance to this PP.

2.3. Package Claim

40 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+.

41 This ST is conforming to assurance package EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3, ALC_DVS.2 defined in CC part 3[CC].

2.4. Conformance rationale

42 Since this ST is not claiming conformance to any other protection profile, and the PP [BACPassPP] is not claiming conformance to another PP, no rationale is necessary here.

2.5. Conformance Statement

43 This ST strictly conforms to [BACPassPP].

3. Security Problem Definition

3.1. Introduction

3.1.1. Assets

44 The assets to be protected by the TOE include the User Data on the MRTD' chip.

Logical MRTD Data

45 The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16(with dierent security needs) and the Document Security Object EF.SOD according to LDS [ICAO-9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the Inspection System for the Chip Authentication and the Active Authentication Public Key (EF.DG15) for Active Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons the 'ICAODoc 9303'[ICAO_9303] specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- LogicalMRTD standardUser Data (i.e. Personal Data) of theMRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16)
- Chip Authentication Public Key in EF.DG14
- Active Authentication Public Key in EF.DG15
- Document Security Object (SOD) in EF.SOD
- Common data in EF.COM

46 A sensitive asset is the following more general one.

Authenticity of the MRTD' chip

47 The authenticity of the MRTD' chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove this possession of a genuine MRTD.

3.1.2. Subjects

48 This protection profile considers the following subjects:

Manufacturer

49 The generic term for the IC Manufacturer producing the integrated circuit and the MRTD

Manufacturer completing the IC to the MRTD’s chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

Personalization Agent

50 The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (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) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [ICAO-9303].

Terminal

51 A terminal is any technical system communicating with the TOE through the contactless interface.

Inspection system (IS)

52 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. **The Basic Inspection System (BIS)** (i) contains a terminal for the contactless communication with the MRTD’s chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. **The General Inspection System (GIS)** is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. **The Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

MRTD Holder

53 The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Traveler

54 Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Attacker

55 A threat agent trying (i) to identify and to trace the movement of the MRTD’s chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Application note 3 : An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.1.3. Assumptions

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

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

57 It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery MRTD delivery during steps 4 to 6

58 Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent Personalization of the MRTD’s chip

59 The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key

(EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection Systems for global interoperability

60 The Inspection System is 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. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

A.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

62 **Application note 4 :** When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

3.2. Threats

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

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

T.Chip_ID **Identification of MRTD's chip**

64 Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: Anonymity of user,

T.Skimming **Skimming the logical MRTD**

65 Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: confidentiality of logical MRTD data

T.Eavesdropping **Eavesdropping to the communication between TOE and inspection system**

66 Adverse action: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: confidentiality of logical MRTD data

T.Forgery **Forgery of data on MRTD's chip**

67 Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat

automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs

Asset: authenticity of logical MRTD data

68 The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

69 Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Information_Leakage Information Leakage from MRTD's chip

70 Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper Physical Tampering

71 Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified.

Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Malfunction Malfunction due to Environmental Stress

72 Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

3.3. Organizational Security Policies

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

P.Manufact Manufacturing of the MRTD's chip

74 The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.Personalization Personalization of the MRTD by issuing State or Organization only

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

P.Personal_Data Personal data protection policy

76 The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)3 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303].

P.Activ_Auth Active Authentication

77 The TOE implements the active authentication protocol as described in [ICAO-9303].

4. Security Objectives

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

4.1. Security Objectives for the TOE

79 This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

80 OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

81 **Application note 5 :** The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

82 OT.Data_Int Integrity of personal data

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

83 OT.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

84 **Application note 6 :** The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO-9303] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this security target. Thus the read access must be prevented even in case of a successful BAC Authentication.

85 **OT.Identification Identification and Authentication of the TOE**

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

86 **Application note 7 :** The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is

identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

87 **OT.Active_Auth_Proof Proof of MRTD's chip authenticity by AA**

The TOE must support the Basic Inspection Systems 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 [ICAO-9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

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

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

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

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

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

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

91 **Application note 8 :** This security objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

Details correspond to an analysis of attack scenarios which is not given here.

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

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data) with a prior
- reverse-engineering to understand the design and its properties and functions.

93 **OT.Prot_Malfunction** **Protection against Malfunctions**

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

94 **Application note 9 :** A malfunction of the TOE may also be caused using a direct interactionwith elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2. Security Objectives for the Operational Environment

Issuing State or Organization

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

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

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases

4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

97 **OE.MRTD_Delivery** **Protection of the MRTD delivery**

Procedures shall ensure protection of TOE material/information under delivery including the following objectives

- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

98 **OE.Personalization** **Personalization of logical MRTD**

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

99 **OE.Pass_Auth_Sign** **Authentication of logical MRTD by Signature**

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the

Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303].

100 OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

Receving State or Organization

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

102 OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303].

103 OE.Passive_Auth_Verif Verification by Passive Authentication

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

104 **OE.Prot_Logical_MRTD Protection of data from the logical MRTD**

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

105 **OE.Active_Auth_Key_travel-document travel-document Active Authentication key**

1 The issuing State or Organization has to establish the necessary public key infrastructure in order to

(i) generate the travel-document's Active Authentication Key Pair,

(ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and

(iii) support inspection systems of receiving States or Organizations to verify the authenticity of the travel-document's chip used for genuine travel-document by certification of the Active Authentication Public Key by means of the Document Security Object.

4.3. Security Objective Rationale

106 The following table provides an overview for security objectives coverage

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Activ_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verift	OE.Prot_Logical_MRTD	OE.Active Auth Key Travel Document
T.Chip_ID				X										X				
T.Skimming			X											X				
T.Eavesdropping			X															
T.Forgery	X	X						X					X		X	X		
T.Abuse-Func						X						X						
T.Information_Leakage							X											
T.Phys-Tamper								X										
T.Malfunction									X									
P.Manufact				X														
P.Personalization	X			X								X						
P.Personal_Data		X	X															
P.Activ_Auth					X													X
A.MRTD_Manufact										X								
A.MRTD_Delivery											X							
A.Pers_Agent												X						
A.Insp_Sys															X		X	
A.BAC-Keys														X				

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

108 The OSP **P.Personalization** “Personalization of the MRTD by issuing State or Organization only” addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** “Personalization of logical MRTD”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD”. Note the manufacturer equips the TOE with the Personalization Agent Key(s)

according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and management of TSF to the Personalization Agent.

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

110 In addition, the OSP **P.Active_Auth** is countered by chip an identification and authenticity proof required by **OT.Active_Auth_Proof** “Proof of travel document’s chip authenticity by AA” using an 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 Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** “the travel document Authentication Key”.

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

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

113 The threat **T.Forgery** “Forgery of data on MRTD’s chip” addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD“ requires the TOE to limit the write

access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** “Integrity of personal data” and **OT.Prot_Phys-Tamper** “Protection against Physical Tampering”. The examination of the presented MRTD passport book according to **OE.Exam_MRTD** “Examination of the MRTD passport book” shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” and verified by the inspection system according to **OE.Passive_Auth_Verif** “Verification by Passive Authentication”.

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

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

116 The assumption **A.MRTD_Manufact** “MRTD manufacturing on step 4 to 6” is covered by the security objective for the TOE environment **OE.MRTD_Manufact** “Protection of the MRTD Manufacturing” that requires to use security procedures during all manufacturing steps.

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

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

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

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

5. Extended Components Definition

120 This ST uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0084]; others are defined in the protection profile [BACPassPP].

5.1. Definition of the family FAU_SAS

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

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

(Table 5-1) Family FAU_SAS

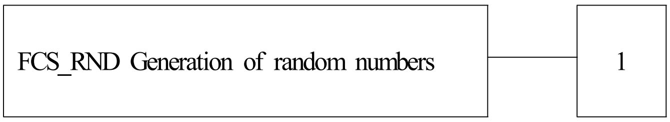
FAU_SAS Audit data storage	
Family behaviour:	This family defines functional requirements for the storage of audit data.
Component leveling:	FAU_SAS Audit data storage 1
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2. Definition of the family FCS_RND

122 To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for noncryptographic use.

The family 'Generation of random numbers (FCS_RND)' is specified as follows:

(Table 5-2) Family FCS_RND

FCS_RND Generation of random numbers	
Family behaviour:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component leveling:	
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

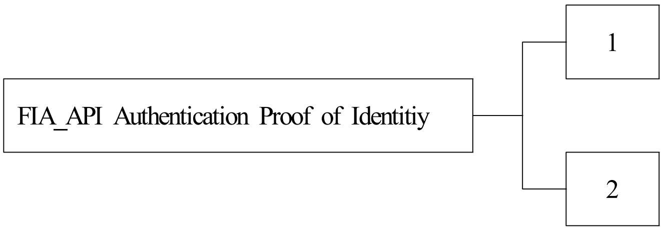
5.3. Definition of the family FMT_LIM

123 The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses

the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

(Table 5-3) Family FMT_LIM

FMT_LIM Limited capabilities and availability	
Family behaviour:	This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
Component leveling:	
FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable

FMT_LIM.1	**Limited capabilities**

Hierarchical to:	No other components
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment:Limited capability and availability policy].

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment:Limited capability and availability policy].

124 **Application Note 10 :** The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

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

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

The combination of both the requirements shall enforce the related policy

5.4. Definition of the family FPT_EMSEC

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

The family ‘TOE Emanation (FPT_EMS)’ is specified as follows:

(Table 5-4) Family FPT_EMSEC

FPT_EMSEC TOE Emanation	
Family behaviour:	This family defines requirements to mitigate intelligible emanations.
Component leveling:	
FPT_EMSEC.1	TOE emanation has two constituents: • FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. • FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable
FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	*No other components*
Dependencies:	*No dependencies.*
FPT_EMSEC.1.1	The TSF shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6. Security Requirements

126 The CC allows several operations to be performed on functional requirements; *refinement, selection, assignment,* and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

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

128 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined text. and the original text of the compnent is given by a footnot. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and underlined text with "<" like <this>.

129 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized with "<" like <*this*>.

130 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

131 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].

(Table 6-1) Definition of security attributes

Security attribute	Values	Meaning
Terminal authentication status	None (any Terminal)	Default role (i.e. without authorisation after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after s uccessful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after succ essful Authentication in accordance with the definition in rul e 1 of FIA_UAU.5.2.

6.1. Security Functional Requirements for the TOE

132 This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1. Class FAU Security Audit

133 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (CC part 2 extended).

FAU_SAS.1 Audit storage

134 Hierarchical to: No other components.

Dependencies: No dependencies

FAU_SAS.1.1	The TSF shall provide the Manufacturer[1] with the capability to store the IC Identification Data[2] in the audit records.

135 **Application Note 11 :** The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the MRTD ma-nufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the MRTD (see

[1] *[assignment: authorized users]*

[2] *[assignment: list of audit information]*

FMT_MTD.1/INI_DIS).

6.1.2. Class FCS Cryptographic Support

136 The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (CC 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/BAC Cryptographic key generation - Generation of Document Basic Access Keys by the TOE

137 Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[3] and specified cryptographic key sizes: 112 bits[4] that meet the following: **[ICAO-9303] Part-11 Section 9.7**[5]

138 **Application Note 12 :** The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO_9303] produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO_9303]. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

FCS_CKM.1/PAC Cryptographic key generation − Generation of PAC session keys

139 Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/PAC	The TSF shall generate cryptographic keys in accordance with a specified

[3] *[assignment: cryptographic key generation algorithm]*
[4] *[assignment: cryptographic key sizes]*
[5] *[assignment: list of standards]*

	cryptographic key generation algorithm : <*Triple-DES or AES key derivation*>[6] and specified cryptographic key sizes: <*112 ,128*>[7], that meet the following: <*[ICAO-9303] Part-11 Section 9.7*>[8]

FCS_CKM.4 Cryptographic key destruction − MRTD

140 The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (CC part 2).

141 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: <*physical deletion by overwriting the memory data with zeros or the new key*>[9] that meets the following: <*none*>[10]

142 **Application Note 13 :** The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

143 The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (CC 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 by MRTD

144 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

[6] *[assignment: cryptographic key generation algorithm]*
[7] *[assignment: cryptographic key sizes]*
[8] *[assignment: list of standards]*
[9] *[assignment: cryptographic key destruction method]*
[10] *[assignment: list of standards]*

FCS_COP.1.1/SHA	The TSF shall perform hashing[11] in accordance with a specific cryptographic algorithm: <SHA-1, SHA-256>[12] and specified cryptographic key sizesd: none[13], that meet the following: <FIPS 180-2>[14],

145 **Application Note 14 :** This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [ICAO-9303], as well as the hash function SHA-256 for the Personalization Agent Authentication Mechanism.

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

146 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption[15] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[16] and cryptographic key sizes 112 bit[17] that meet the following: **[FIPS46-3] and [ICAO-9303], Part-11 Section 9.7**[18].

147 **Application Note 15 :** 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/PAC Cryptographic operation – Symmetric encryption/decryption and MAC during Personalization

148 Hierarchical to : No other components.

[11] [assignment: list of cryptographic operations]
[12] [assignment: cryptographic algorithm]
[13] [assignment: cryptographic key sizes]
[14] [assignment: list of standards]

[16] [assignment: cryptographic algorithm]
[17] [assignment: cryptographic key sizes]
[18] [assignment: list of standards]

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/PAC
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/PAC	The TSF shall perform <*secure messaging (PAC) - symmetric encryption and decryption*>[19] in accordance with a specified cryptographic algorithm <*3-DES, AES*>[20] and cryptographic key sizes <*112, 128 bit*>[21] that meet the following : <*Table 6-2*>[22]

(Table 6-2) Algorithms and key sizes for PAC

Algorithm	Key size	List of standards
TDES encryption and decryption	112 bits	[SP 800-67]
AES encryption and decryption	128 bits	[FIPS 197]
TDES Retail MAC	112 bits	[ISO 9797]
AES CMAC	128 bits	[NIST-SP800-38B]

FCS_COP.1/AUTH Cryptographic operation – Authentication

149 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption[23] in accordance with a specified cryptographic algorithm <Triple-DES and AES>[24] and cryptographic key sizes <**112 bit for Triple-DES and 128 bit for AES**>[25] that meet the following: <**[FIPS 46-3]** and [**FIPS 197**]>[26]

[19] [assignment: list of cryptographic operations]
[20] [selection: AES, 3DES] in CBC mode
[21] [selection: 112, 128]
[22] [assignment: list of standards]
[23] [assignment: list of cryptographic operations]
[24] [assignment: cryptographic algorithm]
[25] [assignment: cryptographic key sizes]

150 **Application Note 16 :** This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC Cryptographic operation − Retail MAC

151 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/MAC	The TSF shall perform secure messaging – message authentication code[27] in accordance with a specified cryptographic algorithm Retail MAC and CMAC[28] and cryptographic key sizes 112 bit for Retail MAC and 128 bit for CMAC[29] that meet the following: **ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) and [NIST_SP800-38B]**[30].

152 **Application Note 17 :** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AA_SIGN Cryptographic operation − Active Autentication

153 Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

[26] [assignment: list of standards]

[27] [assignment: list of cryptographic operations]

[28] [assignment: cryptographic algorithm]

[29] [assignment: cryptographic key sizes]

[30] [assignment: list of standards]

FCS_COP.1.1/ AA_SIGN	The TSF shall perform <*digital signature creation*> in accordance with a specified cryptographic algorithm <*RSA and ECDSA*> and cryptographic key sizes <*2048 bit for RSA and 192, 224, 256, 384, 512 bit for ECDSA*> that meet the following: <*[ISO9796-2] and [ECC-TR]*>.

154 **Application Note 18 :** This SFR has been added by the ST author to specify the cryptographic algorithm and key sizes used by the TOE to perform an Active Authentication in accordance with [ICAO9303-11].

FCS_RND.1 Quality metric for random numbers

155 Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet <*BSI AIS-31 functionality class PTG.2 of German scheme and RGS of French scheme [DTRNG]*>[31].

156 **Application Note 19 :** This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.3. Class FIA Identification and Authentication

157 The following Table provides an overview of the authentication mechanisms used.

(Table 6-3) Overview of authentication SFRs

Mechanism	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303], and [EACTR]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	either Triple-DES with 112 bit keys or AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)
Active Authentication Protocol	FIA_API.1/AA and FIA_UAU.4	ECDSA, 192, 224, 256, 320, 384, and 512 bitsand RSA CRT, 2048 bits

[31] *[assignment: a defined quality metric]*

FIA_AFL.1/PAC Authentication failure handling in Pesonalization

158 Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PAC	The TSF shall detect when <5>[32] unsuccessful authentication attempts occur related to <*consecutive failed authentication attempts with respect to the initialization key*>[33].
FIA_AFL.1.2/PAC	When the defined number of consecutive unsuccessful authentication attempts has been <*met*>[34], the TSF shall <*block the Personalization key and terminate TOE*>[35].

FIA_AFL.1/BAC Authentication failure handling in BAC authenticaion

159 Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/BAC	The TSF shall detect when <2>[36] unsuccessful authentication attempt occurs related to <*BAC authentication*>[37].
FIA_AFL.1.2/BAC	When the defined number of consecutive unsuccessful authentication attempts has been <*met*>[38], the TSF shall <*delay the next authentication attempt at least 10 seconds*>[39]**.**

160 The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (CC part 2).

FIA_UID.1 Timing of identification

161 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 “Manufacturing”,

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

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

[34] *[selection: met or surpassed]*

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

[36] *[assignment: positive integer number]*

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

[38] *[assignment: met or surpassed]*

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

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

	2. to read the random identifier in Phase 3 “Personalization of the MRTD”, 3. to read the random identifier in Phase 4 “Operational Use”[40] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

162 **Application Note 20 :** The IC manufacturer and the MRTD manufacturer write the initialization data and/or pre-personalization data in the audit records of the IC during the phase 2 “Manufacturing” The audit records can be written only in the phase 2 “Manufacturing of the TOE” At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer creates the user role Personalization Agent for transition from phase 2 to phase 3 “Personalization of the MRTD” The users in role Personalization Agent identify themselves by means of selecting the authentication key. Aer personalization in the phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

163 **Application Note 21 :** In the “Operational use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’ chip use a randomly chosen identifier for the communication channel to allow the terminal to communicate with more then one RFID. This identifier will not violate the OT.Identification.

164 The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (CC part 2).

FIA_UAU.1 Timing of authentication

165 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 “Manufacturing”, 2. to read the random identifier in Phase 3 “Personalization of the MRTD”,

	3. to read the random identifier in Phase 4 “Operational Use” on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

166 **Application note 22 :** The Basic Inspection System and the Personalization Agent authenticate themselves.

167 The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (CC part 2).

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

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

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism 2. Authentication Mechanism based on <Triple-DES and AES>[41]

169 **Application Note 23 :** The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

170 **Application Note 24 :** The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO-9303]. In the first step the terminal authenticates itself to the MRTD’ chip and the MRTD’ chip authenticates to the terminal in the second step. In this second step the MRTD’ chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD’ 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.

171 The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (CC part 2).

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

FIA_UAU.5 Multiple authentication mechanisms

172 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1	The TSF shall provide 1. Basic Access Control Authentication Mechanism 2. Authentication Mechanism based on <Triple-DES and AES>[42] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms <the Symmetric Authentication Mechanism with 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[43]

173 **Application note 25 :** In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [EACPassPP] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [EACPassPP] FIA_UAU.5.2).

174 **Application note 26 :** The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

175 The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (CC

[42] *[assignment: list of multiple authentication mechanisms]*
[43] *[assignment: rules describing how the multiple authentication mechanisms provide authentication]*

part 2)

FIA_UAU.6 Re-authenticating − Re-authenticating of Terminal by the TOE

176 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism[44].

177 **Application note 27 :** The Basic Access Control Mechanism specified in [ICAO-9303] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

178 **Application note 28 :** Note that in case the TOE should also fulfill [EACPassPP] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

179 The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (CC part 2 extended).

FIA_API.1/AA Authentication Proof of Identity - Active Authentication

180 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA	The TSF shall provide an <*Active Authentication Protocol according to [ICAO-9303]*> to prove the identity of the <*TOE*>**.**

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

181 **Application Note 29 :** This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generate a challenge then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corrensponding to the Active Authentication public key (EF.DG.15)

6.1.4 Class FDP User Data Protection

182 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria part 2).

FDP_ACC.1 Subset access control - Basic Access Control

183 Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP[45] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[46]

184 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (CC part 2).

FDP_ACF.1 Security attribute based access control

185 Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Personalization Agent, b. Basic Inspection System, c. Terminal,

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

[46] *[assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]*

	2. Objects: a. data EF.DG1 to EF.DG16 of the logical MRTD, b. data in EF.COM, c. data in EF.SOD, **3.** Security attributes: a. authentication status of terminals[47].
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[48].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[49]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical 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.[50].

186 **Application Note 30 :** The inspection system needs special authentication and authorization for read access to DG3 and DG4 defined in [EACPassPP].

187 The TOE shall meet the requirement “Basic data exchange integrity (FDP_UIT.1)” as specified below (CC part 2).

[47] [assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

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

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

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

FDP_UIT.1 Data exchange integrity - MRTD

188 Hierarchical to: No other components.

Dependencies: [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]

FDP_UIT.1.1	The TSF shall enforce the Basic Access Control SFP[51] to be able to transmit and receive[52] user data in a manner protected from modification, deletion, insertion and replay[53] errors
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[54] has occurred.

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

FDP_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1	The TSF shall enforce the Basic Access Control SFP[55] to be able to transmit and receive[56] user data in a manner protected from unauthorised disclosure

6.1.4. Class FMT Security Management

190 The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

[51] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[52] [selection: transmit, receive]
[53] [selection: modification, deletion, insertion, replay]
[54] [selection: modification, deletion, insertion, replay]
[55] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[56] [selection: transmit, receive]

191 The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (CC part 2).

FMT_SMF.1 Specification of Management Functions

192 Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-Personalization, 3. Personalization[57]

193 The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (CC part 2).

FMT_SMR.1 Security roles

194 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	The TSF shall maintain the roles: 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System[58]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

195 **Application Note 31 :** The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

196 The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below(CC part 2 extended).

FMT_LIM.1 Limited capabilities

197 Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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

[58] *[assignment: the authorized identified roles]*

FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks

6.1.6.4 FMT_LIM.2 Limited availability

198 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (CC part 2 extended).

FMT_LIM.2 Limited availability

199 Hierarchical to: No other components.
Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks

200 **Application note 32 :** The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

201 **Application Note 33 :** the following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

FMT_MTD.1/INI_ENA Management of TSF data − Writing of Initialization Data and Pre-personalization Data

203 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[59] the Initialization Data and Pre-personalization Data[60] to the Manufacturer[61].

204 **Application note 34 :** The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric ryptographic Personalization Agent Key.

FMT_MTD.1/INI_DIS Management of TSF data − Disable of Read Access to Initialisation Data and Pre-personalization Data

205 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to disable read access for users to[62] the Initialization Data[63] to the Personalization Agent[64]

206 **Application Note 35 :** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users

[59] *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
[60] *[assignment: list of TSF data]*
[61] *[assignment: the authorised identified roles]*
[62] *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
[63] *[assignment: list of TSF data]*
[64] *[assignment: the authorised identified roles]*

within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_WRITE Management of TSF data − Key Write

207 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to write[65] the Document Basic Access Keys[66] to the Personalization Agent[67]

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

208 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read[68] the 1. Document Basic Access Keys 2. Personalization Agent Keys[69] 3. **Active Authentication Private Key** to none[70]

209 **Application note 36 :** The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

[65] *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
[66] *[assignment: list of TSF data]*
[67] *[assignment: the authorized identified roles]*
[68] *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
[69] *[assignment: list of TSF data]*
[70] *[assignment: the authorized identified roles]*

FMT_MTD.1/AAPK Management of TSF data − Active Authentication Private Key

210 Hierarchical to: No other components.

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

FMT_SMR.1 Security roles

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to <*load*>[71] the <*Active Authentication Private Key*>[72] to the <*Personalization Agent*>[73]

FMT_MTD.1/PAC_KEY Management of TSF data − Updating of PAC Key

211 Hierarchical to: No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/PAC_KEY	The TSF shall restrict the ability to <*modify*>[74] the <*PAC Authentication key*>[75] to the <*Personalization Agent*>[76]

6.1.5. Class FPT Protection of the Security Functions

212 The TOE shall prevent inherent and forced illicit information leakage for User Data and TSFdata.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 security functionality.

213 The TOE shall meet the requirement “TOE emanation (FPT_EMS.1)” as specified below (CC part 2 extended):

[71] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[72] [assignment: list of TSF data]
[73] [assignment: the authorised identified roles]
[74] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[75] [assignment: list of TSF data]
[76] [assignment: the authorised identified roles]

FPT_EMSEC.1 TOE Emanation

214 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1	The TOE shall not emit <*power variations, timing variations during command execution*>[77] in excess of <*non-useful information*>[78] enabling access to 1. Personalizastion Agent Keys(s) and 2. <*Document Basic Access Keys*>, 3. <*Active Authenticate Private Keys*>[79]
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users[80] are unable to use the following interface smart card circuits contacts[81] to gain access to 1. Personalizastion Agent Keys(s) and 2. <*Document Basic Access Keys*>, 3. <*Active Authenticate Private Keys*>[82]

215 **Application Note 37** : The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contact according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

217 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)"

[77] *[assignment: list of audit information]*
[78] *[assignment: types of emissions]*
[79] *[assignment: list of types of user data].*
[80] *[assignment: type of users]*
[81] *[assignment: type of connection]*
[82] *[assignment: list of types of user data].*

as specified below (CC part 2).

FPT_FLS.1 Failure with preservation of secure state

218 Hierarchical to: No other components.

Dependencies: No dependencies

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur 2. Failure detected by TSF according to FPT_TST.1

219 The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (CC part 2).

FPT_TST.1 TSF testing

220 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1	The TSF shall run a suite of self tests <during initial start-up, periodically during normal operation, *<during cryptographic computation and before any use of TSF data>*>[83] to demonstrate the correct operation of the TSF[84].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[85].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

221 **Application Note 38 :** During initial start-up RNG live test, it runs sensor test and Fault Attack detection and performs periodically monitoring of Fault Attack detection module and RNG H/W module. It also runs various Fault Attack detection before and after crypto operation and verification of integrity by calculating checksum value before using TSF data strored in protective memory.

[83] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]

[84] [selection: [assignment: parts of TSF], the TSF]

[85] [selection: [assignment: parts of TSF], TSF data]

222 **Application Note 39 :** If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

223 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (CC part 2).

FPT_PHP.3 Resistance to physical attack

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

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[86] to the TSF[87] by responding automatically such that the SFRs are always enforced.

225 **Application Note 40 :** The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

[86] *[assignment: physical tampering scenarios]*
[87] *[assignment: list of TSF devices/elements]*

6.2. Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

● ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2, ATE_DPT.3 and ALC_DVS.2.

(Table 6-4) summarizes the assurance components that define the security assurance requirements for the TOE.

Assurance Class	Assurance Components
ADV	ADV_ARC.1 ADV_FSP.5 ADV_IMP.1 ADV_INT.2 ADV_TDS.4
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.4 ALC_CMS.5 ALC_DEL.1 ALC_DVS.2 ALC_LCD.1 ALC_TAT.2
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
ATE	ATE_COV.2 ATE_DPT.3 ATE_FUN.1 ATE_IND.2
ADV	AVA_VAN.3

6.3. Security Requirements Rationale

6.3.1. Security functional requirements rationale

(Table 6-5) Coverage of Security Objective for the TOE by SFR

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func	OT.Active_Auth_Proof
FAU_SAS.1				X					
FCS_CKM.1/BAC	X	X	X						
FCS_CKM.1/PAC	X	X	X						
FCS_CKM.4	X		X						
FCS_COP.1/SHA	X	X	X						
FCS_COP.1/ENC	X	X	X						
FCS_COP.1/PAC	X	X	X						
FCS_COP.1/MAC	X	X	X						
FCS_COP.1/AUTH	X	X							
FCS_COP.1/AA_SIGN									X
FCS_RND.1	X	X	X						
FIA_AFL.1/PAC			X	X					
FIA_AFL.1/BAC			X	X					
FIA_UID.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						
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/PAC_KEY	X	X							
FMT_MTD.1/AAPK		X							X
FPT_EMSEC.1	X				X				
FPT_TST.1					X		X		
FPT_FLS.1	X				X		X		
FPT_PHP.3	X				X	X			

227 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. PAC key for authentication between Personalization Agent and TOE can be updated according to SFR FMT_MTD.1/PAC_KEY.

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

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

The SFR FCS_CKM.1/PAC and FCS_COP.1/PAC allows to protect the transmitted data by means secure messaging during the presonalization processes.

228 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). PAC key for authentication between Personalization Agent and TOE can be updated according to SFR FMT_MTD.1/PAC_KEY. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical 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/BAC, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The SFR FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Active Authentication Key cannot be written unauthorized or read afterwards.

In personalization, the SFR FCS_CKM.1/PAC and FCS_COP.1/PAC ensure the authenticity of data transfers after successful authentication of the personalization agent.

229 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/BAC 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/BAC, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys. Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

In personalization, the SFR FCS_CKM.1/PAC and FCS_COP.1/PAC ensure the confidentiality of data transfers after successful authentication of the personalization agent according to FIA_UID.1 and FIA_UAU.1 with the support of FIA_AFL.1/PAC.

230 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 (cf. Application note 24). In case of failed authentication attempts FIA_AFL.1/BAC, enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

In case of failed authentication attempts FIA_AFL.1/PAC block the authentication key

231 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

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

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

233 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.

234 The security objective **OT.Active_Auth_Proof** “Proof of MRTD’s chip authenticity through AA” addresses the verification of the chip's authenticity. This done by the SFR FIA_API.1/AA which authenticates the chip, using cryptographic operations covered by the SFR FCS_COP/AA_SIGN. The Active Authentication Protocol is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ.

6.3.2. Dependency Rationale

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

236 Table 6-6 shows the dependencies between the SFR of the TOE.

(Table 6-6) Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/BAC	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC Fulfilled by FCS_CKM.4
FCS_CKM.1/PAC	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/AUTH and FCS_COP.1/PAC Fulfilled by FCS_CKM.4
FCS_CKM.4	[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/BAC and FCS_CKM.1/PAC
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 1 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/BAC Fulfilled by FCS_CKM.4
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attrib	Fulfilled by FCS_CKM.1/BAC

	utes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/PAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/PAC Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 2 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/AA_SIGN	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 5 for non-satisfied dependencies
FCS_RND.1	No dependencies	
FIA_AFL.1/PAC	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/BAC	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	
FIA_UAU.1	FIA_UID.1 Timing of identfication	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_API.1/AA	No dependencies	
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1 justification 3 for nonsatisfied dependencies
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 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control orFDP_IFC.1 Subset information flow control]	Justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1

FMT_SMF	No dependencies	
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/PAC_KEY	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	

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

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

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

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

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the 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 channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

No. 5: Since AA doesn’t provide for generation or destruction of cryptographic keys, the

FCS_CKM.4, FCS_CKM.1 doesn't apply

6.3.3. Security Assurance Requirements Rationale

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

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

The component ALC_DVS.2 has no dependencies.

Notice that it the augmentation components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 come from the EAL5 level.

6.3.4. Secuirty Requirements – Mutual Support and Internal Consistency

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

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

The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7. TOE Summary Specification

240 The following sections provide a general understanding of how the TOE is implemented. This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

7.1. TOE Security Functions

241 This chapter gives the overview description of the different TOE Security Functions composing the TSF.

(Table 7-1) TOE Security Feature

Security Feature	Description
SF.IC	IC chip security feature
SF.PAC_AUTH	PAC authentication and creation of PAC session key
SF.BAC_AUTH	BAC authentication and creation of BAC session key
SF.ACTIVE_AUTH	AA authentication
SF.SEC_MESSAGE	Secure messaging
SF.ACC_CONTROL	TSF Access control
SF.RELIABILITY	Protection against Physical Manipulation, TSF selftest, Integrity check

7.1.1. SF.IC

242 The TOE uses TSFs provided by IC chip to enforce security. Refer to documents related to IC chip for details of TSF of the IC chip [HWST].

7.1.2. SF.PAC_AUTH

243 This TSF includes the PAC authentication mechanism for Personalization Agent, the PAC authentication mechanism provides authority control of the security role to the Personalization Agent in the personalization phase. It is composed of PAC Initialization, PAC mutual authentication and PAC session key generation.

- **PAC Initialization**

244 During the PAC Initialization, TOE generates key encryption key(KEK), initializes the file table for LDS filesystem. By performing PAC Initialization, the initialization parameters including PAC authentication key are securely loaded to TOE and the state transition from Empty to Unissue has occurred. PAC Initialization can be performed only once and the state transition from Unissue to Empty is irreversible.

- **PAC mutual authentication**

245 TOE and Personalization Agent authenticate mutually each other. Personalization Agent sends the data to the TOE, then TOE authenticates the Personalization Agent by performing a MAC verification and comparison received cryptographic value. Then TOE sends cryptographic value to the Personalization Agent and Personalization Agent can ensure that TOE is the authenticated one by performing a MAC verification and comparison response cryptographic value.

- **PAC session key generation**

246 After successfully PAC mutual authentication, PAC session keys are generated to establish secure communication channel between TOE and Personalization Agent. The User data and TSF data should be personalized to TOE by means of secure messaging with PAC session keys.

7.1.3. SF.BAC_AUTH

247 If the Inspection System does not perform SAC mechanism, it performs BAC mechanism. The BAC security mechanism(Basic Access Control) provides confidentiality and integrity for the personal data of the ePassport holder via secure messaging when controlling access to the personal data of the ePassport holder records in the TOE and transmitting it to the Inspection System with read-rights. This TSF is composed of BAC mutual authentication and BAC session key generation.

7.1.4. SF.ACTIVE_AUTH

248 This TSF provides an AA mechanism with which the TOE verifies that the MRTD chip is genuine to the Inspection System by signing the random number transmitted from the Inspection System; the Inspection System verifies the authenticity of the MRTD chip through verification

with the signed values. In personalization phase AA private key is written into the TOE's securely protected area and public key is stored into DG15.

7.1.5. SF.SEC_MESSAGE

249 This TSF provides a secure communication channel to protect the command message(C-APDU) and response message(R-APDU) between the TOE and the Personalization Agent or the Inspection System. The secure communication channel means that between TOE and Personalization Agent, that between TOE and Inspection System.

7.1.6. SF.ACC_CONTROL

250 This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. The TOE provides access control rules and management functions for the ePassport application data based on security.

7.1.7. SF.RELIABILITY

251 This TSF executes the residual information management, ensures that any information content of the related crypto is made unavailable. It also performs self-test, provides integrity check, preserves the secure protection when case of abnormal operation and provides countermeasure from physical invasion. etc..

8. Reference

8.1. Acronyms

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CAN	Card Access Number
CBC	Cipher-block Chaining (block cipher mode of operation)
CC	Common Criteria
COM	Common data group of the LDS (ICAO Doc 9303-10)
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO Doc 9303-10)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
IC	Integrated Circuit
IS	Inspection System
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone

N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PACE	Password Authenticated Connection Establishment
PACE-GM	PACE with Generic Mapping
PACE-IM	PACE with Integrated Mapping
PACE-CAM	PACE with Chip Authentication Mapping
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAC	Supplemental Access Control
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOD	Document Security Object
SPA	Simple Power Analysis
ST	Security Target
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TR	Technical Report
VIZ	Visual Inspection Zone

8.2. Glossary

Accurate Terminal Certificate A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document''s chip to produce Terminal Certificates with the correct certificate effective date, see [EAC-TR].

Advanced Inspection Procedure (with PACE) A specific order of authentication steps between a travel document and a terminal as required by [ICAO_SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE and EIS-AIP-BAC.

Agreement This term is used in BSI-CC-PP-0056-V2-2011 [PACEPassPP] in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.

Active Authentication Security mechanism defined in [ICAO-9303] option by which means the travel document''s chip proves and the inspection system verifies the identity and authenticity of the travel document''s chip as part of a genuine travel document issued by a known State of Organization.

Application note / Note Optional informative part of the ST containing sensitive supporting information hat is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records Write-only-once non-volatile memory area of the travel document''s chip to store the Initialization Data and Pre-personalization Data.

Authenticity Ability to confirm the travel document and its data elements on the travel document''s chip were created by the issuing State or Organization

Basic Access Control (BAC) Security mechanism defined in [ICAO-9303] by which means the travel document''s chip proves and the basic inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

Basic Inspection System with PACE protocol (BIS-PACE) A technical system being used by an inspecting authority and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).

The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorized by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.

Basic Inspection System (BIS) An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document"s chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.

Biographical data (biodata) The personalized details of the travel document holder 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. [ICAO-9303]

Biometric reference data Data stored for biometric authentication of the travel document holder in the travel document"s chip as (i) digital portrait and (ii) optional biometric reference data.

Card Access Number (CAN) Password derived from a short number printed on the front side of the data-page.

Certificate chain A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO-9303]

Country Signing CA Certificate (CCSCA) Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the inspection system.

Country Signing Certification Authority (CSCA) An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see.

[ICAO-9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC-TR].

Country Verifying Certification Authority (CVCA) An organization enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EAC-TR].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a CVCS as a subject; hence, it merely represents an organizational entity within BSI-CC-PP-0056-V2-2012.

The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC-TR].

Current date The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CV Certificate Card Verifiable Certificate according to [EAC-TR].

CVCA link Certificate Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

PACE passwords Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-9303].

Document Details Data Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.

Document Security Object (SOD) A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document''s chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]

Document Signer (DS) An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.

A Document Signer is authorized by the national CSCA issuing the Document SignerCertificate (CDS)(CDS), see [EAC-TR] and [ICAO-9303].

This role is usually delegated to a Personalization Agent.

Document Verifier (DV) An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State''s border police), by - inter alia - issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [EAC-TR].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity within this ST.

There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer and a foreign CVCA ensuring enforcing the travel document Issuer''s privacy policy).1,2

Eavesdropper A threat agent with high attack potential reading the communication between the travel document''s chip and the inspection system to gain the data on the travel document''s chip.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person''s identity. [ICAO-9303]

Travel document (electronic) The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

ePassport application A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [EAC-TR].

Extended Access Control Security mechanism identified in [ICAO-9303] by which means the travel document"s chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.

Extended Inspection System (EIS) A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or 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 portrait. [ICAO-9303]

Global Interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all travel documents. [ICAO-9303]

IC Dedicated Software Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players.

The form of such an agreement may be of formal and informal nature; the term "agreement" is used in BSICC-PP-0068-V2-2011 in order to reflect an appropriate relationship between the parties involved.

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

The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.

IC Dedicated Support Software That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC Embedded Software Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.

IC Identification Data The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person''s document. [ICAO-9303]

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. [ICAO-9303]

Initialization Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).

Initialization Data Any data defined by the TOE manufacturer and injected into the nonvolatile memory by the Integrated Circuits manufacturer (Phase 2). These data are, for instance, used for traceability and for IC identification as travel document''s material (IC identification data).

Inspection The act of State examining an travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO-9303].

Inspection system (IS) A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder.

Integrated circuit (IC) Electronic component(s) designed to perform processing and/or memory functions. The travel document''s chip is an integrated circuit.

Integrity Ability to confirm the travel document and its data elements on the travel document''s chip have not been altered from that created by the issuing State or Organisation.

Issuing Organization Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]

Issuing State The Country issuing the travel document. [ICAO-9303]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the travel document''s chip.

Logical travel document Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to)

1. personal data of the travel document holder
2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
3. the digitized portraits (EF.DG2),
4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and
5. the other data according to LDS (EF.DG5 to EF.DG16).
6. EF.COM and EF.SOD

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. [ICAO-9303].

Machine readable zone (MRZ) Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1,the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303].

The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]

Manufacturer Generic term for the IC manufacturer producing integrated circuit and the travel document manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC manufacturer and travel document manufacturer using this role manufacturer.

Metadata of a CV Certificate Data within the certificate body (excepting Public Key) as described in [EAC-TR].

The metadata of a CV certificate comprise the following elements:

- Certificate Profile Identifier,
- Certificate Authority Reference,
- Certificate Holder Reference,
- Certificate Holder Authorization Template,
- Certificate Effective Date,
- Certificate Expiration Date.

ePassport application Non-executable data defining the functionality of the operating system on the IC as the travel document"s chip. It includes

- the file structure implementing the LDS [ICAO-9303],
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except the authentication data itself.

Optional biometric reference data Data stored for biometric authentication of the travel document holder in the travel document"s chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication Security mechanism implementing (i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Password Authenticated Connection Establishment (PACE) A communication establishment protocol defined in [ICAO-9303]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password ¼). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.

PACE password A password needed for PACE authentication, e.g. CAN or MRZ.

Personalization The process by which the Personalization Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the “"Enrollment”" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).

Personalization Agent An organization acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities:

i establishing the identity of the travel document holder for the biographic data in the travel document,

ii enrolling the biometric reference data of the travel document holder,

iii writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [EAC-TR],

iv writing the document details data,

v writing the initial TSF data,

vi signing the Document Security Object defined in [ICAO-9303] (in the role of DS).

Please note that the role ”Personalization Agent” may be distributed among several institutions according to the operational policy of the travel document Issuer.

Generating signature key pair(s) is not in the scope of the tasks of this role.

Personalization Data A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the life cycle phase card issuing.

Pre-personalization Data Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalized travel document and/or to secure shipment within or between the life cycle phases Manufacturing and card issuing.

Pre-personalized travel document"s chip Travel document"s chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.

Receiving State The Country to which the travel document holder is applying for entry; see [ICAO-9303].

Reference data Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

RF-terminal A device being able to establish communication with an RF-chip according to ISO/IEC 14443.

Rightful equipment (rightful terminal or rightful Card) A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see Inspection System).

Secondary image A repeat image of the holder"s portrait reproduced elsewhere in the document by whatever means; see [ICAO-9303]

Secure messaging in combined mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Skimming Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed PACE password.

Standard Inspection Procedure A specific order of authentication steps between an travel document and a terminal as required by [ICAO-9303], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.

Supplemental Access Control A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.

Terminal A Terminal is any technical system communicating with the TOE through a contactless/contact interface.

TOE tracing data Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognizing the travel document.

Travel document Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there “"Machine readable travel document”").

Travel document (electronic) The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

Travel document holder A person for whom the ePass Issuer has personalized the travel document.

Travel document Issuer (issuing authority) Organization authorized to issue an electronic Passport to the travel document holder.

Travel document presenter A person presenting the travel document to a terminal and claiming the identity of the travel document holder.

TSF data Data created by and for the TOE that might affect the operation of the TOE ([CC]-Part1).

Unpersonalized travel document Travel document material prepared to produce a personalized travel document containing an initialized and pre-personalized travel document''s chip.

User data All data (being not authentication data)

i stored in the context of the ePassport application of the travel document as defined in [ICAO-9303] and

ii being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-9303]).

CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF ([CC]-Part1). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning ([CC]-Part2).

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.

8.3. Technical References

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security Functional Requirements; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security Assurance Requirements; Version 3.1, April 2017, CCMB-2017-04-003
Common Methodology for Information Technology Security Evaluation, Evaluation Metho-dology, Version 3.1, April 2017, CCMB-2017-04-004

[EAC-TR]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents,
Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015,
Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), BSI, Version 2.21, 2016-12,
Part 3 - Common Specifications, BSI, Version 2.21, 2016-12

[ICAO-9303]

ICAO Doc 9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 1-12

[ECC-TR]

Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06

[BACPassPP]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, BSI-CC-PP-0055, Bundesamt füur Sicherheit in der Informa-tionstechnik (BSI), 2009-03-25

[PACEPassPP]

CC Protection Profile: Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP- 0068-V2-2011, 2011-11-02

[EACPassPP]

CC Protection Profile: Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, Version 1.3.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP- 0056-V2-2012, 2012-12-05

[RSA-PKCS#1]

PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.

[SP 800-67]

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2012

[RSA-PKCS#3]

PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.

[FIPS186]

Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07

[RFC5639]

M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[ISO_9796-2]

ISO/IEC 9796-2:2002, Information technology – Security techniques –
Digital signature schemes giving message recovery – Part 2: Integer factorization
based mechanisms, ISO/IEC, 2008-03.

[HWCR]

Certification Report of S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A ANSSI-CC-2019/01

[HWST]

Security Target of S3D350A/S3D300A/S3D264A/S3D232A/S3D200A/S3K350A/S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, Version 4.1, 25 OCT 2018.

[DTRNG]

S3D350A/S3K1170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note, 2017.10.12., Rev1.6

[FIPS_197]

FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001-11-26.

[ISO_9797]

ISO/IEC 9797:1999, 2002, Information technology –- Security techniques –- Message Authentication Codes (MACs) –- Multipart Standard, ISO/IEC, 1999, 2002.

[NIST_SP800-38B]

NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2005-05.

[ISO 11770-3]

Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, 2015.