ID&TRUST

IDENTITY APPLET V4.0/BAC/AA EPASSPORT WITH BAC AND ACTIVE AUTHENTICATION SECURITY TARGET

COMMON CRITERIA / ISO 15408

EAL4+

2026

Revision history

Version	Date	Information
V1.0	12.01.2026	First release

Table of Contents

1. ST Introduction

This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils its requirements.

Throughout this document, the term BAC refers to Basic Access Control.

The inspection system SHALL use BAC in the session.

The TOE is a composite TOE. The Common Criteria Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices [9] contains all the relevant information about the methodology to handle such a TOE. The developer followed the direction of the mandatory document, and so should any relevant parties participate in the evaluation and certification of the TOE.

1.1. ST reference

Title:	Security Target IDentity Applet v4.0/BAC/AA – ePassport with BAC and Active Authentication
TOE:	IDentity Applet v4.0/BAC on NXP JCOP 4.5 P71
Author:	ID&Trust Ltd.
Version Number:	v1.0
Date:	12.01.2026

1.2. TOE reference

The Security Target refers to the product “ID&Trust IDentity Applet Suite v4.0” for CC evaluation.

TOE Name:	IDentity Applet v4.0/BAC on NXP JCOP 4.5 P71
TOE short name:	IDentity Applet v4.0/BAC
TOE Identification Data:	IDentity Applet/BAC v4.0.9219
Platform Identification Data:	
Patch ID	0000000000000000
ROM ID	B3375FE9B5508BC4
Build ID	6D20B6197D635E7C
Platform ID	J3R6000373181200

The TOE name and the TOE identification data constitute the accurate TOE reference.

Evaluation Criteria:	[4]
Evaluation Assurance Level:	EAL 4 augmented with ALC_DVS.2

Developer: ID&Trust Ltd.

Evaluation Sponsor: NXP Semiconductors Netherlands B.V. 5656, AG Eindhoven, High Tech Campus 60

1.3. TOE overview

1.3.1. TOE definition

The TOE comprises:

I. Underlying platform of the TOE, which is evaluated by SGS Brightsight and certified by TÜV Rheinland Nederland B.V. at assurance level

Evaluation assurance level: EAL6 augmented by ASE_TSS.2 and ALC_FLR.1.

CC Certification number: NSCIB-CC-2300127-02

Long platform name: JCOP 4.5 P71

Short name: JCOP 4.5

It consists of:

a) Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);
b) IC Dedicated Software (MC FW Micro Controller Firmware and Crypto Library);
c) IC Embedded Software JCOP 4.5 (Java Card Virtual Machine, Runtime Environment, Java Card API;
d) Global Platform (GP) Framework;

II. the Application Part of the TOE:

ID&Trust IDentity Applet Suite v4.0/BAC;

III. the associated guidance documentation [5], [6].

The PP-0055 [17] refers to the TOE as MRTD, Machine Readable Travel Documents or Travel Document. In order to facilitate the better usage, the terminology is not changed in the current ST.

1.3.2. TOE usage and major security features

The TOE is a contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP 4.5) and IDentity Applet v4.0/BAC, containing components for a machine readable travel document (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to [9] and [13] and optionally Active Authentication defined by [13].

IDentity Applet Suite v4.0 is a highly configurable eID solution. It is able to satisfy multiple different application requirements even within a single applet instance. The Application part of the TOE, the applet functionalities are distributed according to the following table:

Application	Function	Standard	Protection Profile
IDentity/PKI	Flexible PKI token	CEN TS 14890-1/2 IAS-ECC 1.0.1 [24]	-

Application	Function	Standard	Protection Profile
IDentity/IAS	European card for e-Services and National e-ID applications	CEN/TS 15480-2 [23] IAS-ECC 1.0.1[24]	-
IDentity/QSCD	Qualified Signature Creation Device	CEN/TS 15480-2 [23] IAS-ECC 1.0.1 [24] REGULATION (EU) No 910/2014 [25]	[20] [21] [33]
IDentity/IDL	International Driving License	ISO/IEC 18013	BSI-CC-PP-0055 [17]
IDentity/EDL	European Driving License	2012/383/EC	-
IDentity/eVR	Electronic Vehicle Registration	1999/37/EC	-
IDentity/eHC	Electronic Health Insurance	CEN/CWA 15794	-
IDentity/BAC	Basic Access Control (BAC)	ICAO Doc 9303 [13]	BSI-CC-PP-0055 [17]
IDentity-J	Basic Access Control (BAC) Password Authenticated Connection Establishment (PACE)	ICAO Doc 9303 [13]	JISEC500 [30] JISEC499 [31]
IDentity/PACE-EAC1	Password Authenticated Connection Establishment (PACE) Extended Access Control v1 (EAC1)	ICAO Doc 9303 [13] ICAO TR-SAC[14] BSI TR-03110 v2.21 [9], [10],[11], [12]	BSI-CC-PP-0068-V2-2011 [19] BSI-CC-PP-0056-V2-2012 [18]
IDentity/eIDAS	Password Authenticated Connection Establishment (PACE) Extended Access Control v1 (EAC1) Extended Access Control v2 (EAC2) Restricted Identification	ICAO TR-SAC[14] BSI TR-03110 v2.21 [9], [10],[11], [12]	BSI-CC-PP-0087 [22]

Table 1 IDentity Applet Suite v4.0 functionalities

All the functions are supplied by the applet "ID&Trust IDentity Suite Version 4.0", the behaviour of the applet changes according to the configuration applied during the personalization phase and the environmental behaviour of the usage phase.

The scope of the current ST is only concerned with applet behaviour of configuration IDentity/BAC.

For the TOE, beside the eMRTD application other applications may be present on the JCOP 4.5. They are not relevant for the current ST and do not infer the Security Functions of the TOE. The TOE utilizes the evaluation of the underlying JCOP 4.5.

The intended customer of the product is the Card Issuer, who is in charge of the issuance of the product to the smartcard holders.

Application note 1 (ST author)

Operational mode of the TOE depends on the decided operation of the Inspection System. IDentity Applet can work using BAC or PACE with EAC authentication also. If the Inspection System uses PACE with EAC, the TOE supports it. Nevertheless, this ST addresses the Basic Access Control only. PACE with EAC is out of the scope of this ST, and it is described in another ST.

1.3.3. TOE Type

The TOE is a contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP 4.5) and IDentity Applet v4.0/BAC.

1.3.4 Non-TOE hardware/software/firmware

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE

1.4. TOE description

1.4.1. Product type

The TOE is a contact based/contactless integrated circuit chip with IC Dedicated Software (Micro Controller Firmware, Crypto Library), Embedded Software (JCOP 4.5) and IDentity Applet v4.0/BAC, viewed as unit of

1) 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.
2) the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [13] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder
   a) the digital Machine-Readable Zone Data (digital MRZ data, EF.DG1),
   b) the digitized portraits (EF.DG2),
   c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
   d) the other data according to LDS (EF.DG5 to EF.DG16) and
   e) the Document Security Object (SOD).

Application note 2 (ST author)

The biometric reference data (EF.DG3 and EF.DG4) are optional according to [13]. If the issuing State or Organisation uses this option, it should protect these data by means of Extended Access Control (EAC1). EAC1 is out of scope of this ST and is described in another ST.

According to the current ST the TOE prevents read access to sensitive User Data (the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4)).

1.4.2. Components of the TOE

Micro Controller

The Micro Controller is a secure smart card controller from NXP from the SmartMX3 family. The Micro Controller contains a co-processor for symmetric cipher, supporting DES operations and AES, as well as an accelerator for asymmetric algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory.

Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

IC dedicated software - Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to non-volatile memory.

IC dedicated software - Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

Micro Controller, IC dedicated software (Micro Controller Firmware, Crypto Library) are covered by the following certification:

Certification ID:	BSI-DSZ-CC-1149-V4-2025
Evaluation level:	EAL6+ ALC_FLR.1 and ASE_TSS.2 according to Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-00084-2014.

IC Embedded Software

Certification ID: NSCIB-CC-2300127-02

JCOP 4.5 consists of Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Global Platform (GP) framework, Configuration Module, etc.

OS Name:	JCOP 4.5 Operating System
Applied OS configuration:	SECID
Product Identification:	Platform ID = J3R6000373181200 ROM ID = B3375FE9B5508BC4
Evaluation Level:	CC EAL 6+ with ASE_TSS.2, ALC_FLR.1 according to Java Card System – Open Configuration Protection Profile, version 3.0.5, Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-PP-0099-2017).

Platform UGD: [27]

IDentity Applet – accomplishing IDentity application

Product name: ID&Trust IDentity Applet Suite

Version: 4.0

Applet name:[1] IDentity Applet V4.0/BAC ePassport with BAC and Active Authentication

TOE Guidance Documentation:[2] IDentity Applet Suite v4.0 Administrator's Guide [5]

IDentity Applet Suite v4.0 User's Guide [6]

The composite part always means IDentity Applet v4.0/BAC

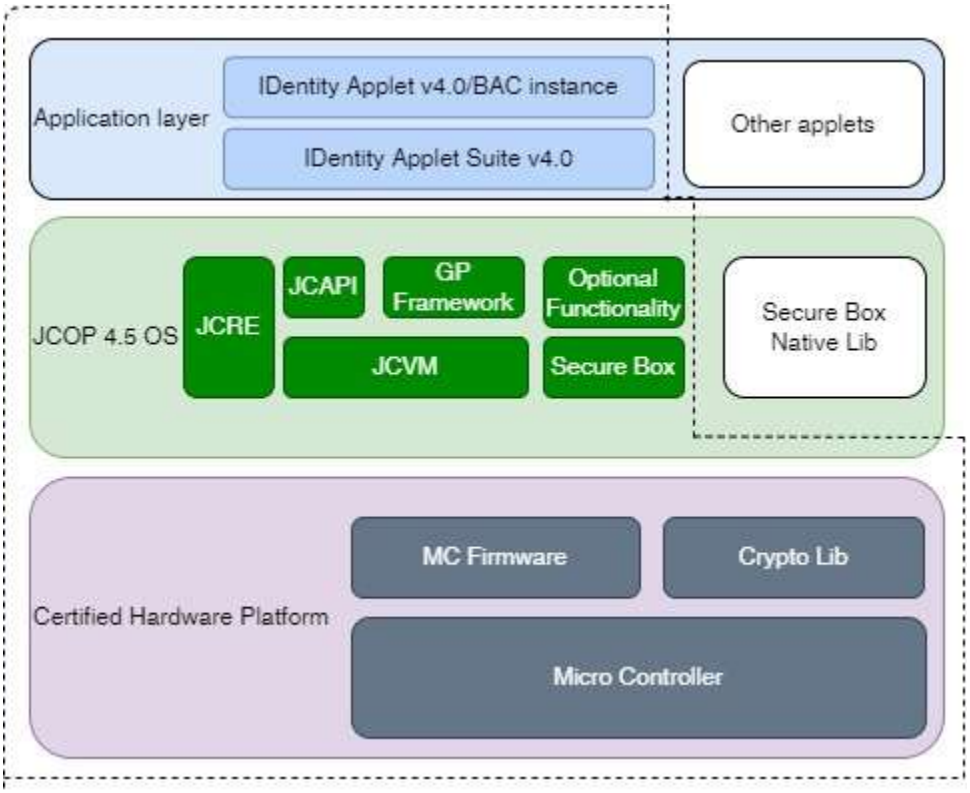

Figure 1 TOE Boundaries

The TOE is a composite TOE, and the dashed line denotes the whole TOE. The underlying certified hardware platform and JCOP 4.5 OS are marked with purple and green. In this ST the common short name of certified hardware platform and JCOP 4.5 OS is Platform.

The blue box marks the application layer. The ID&Trust IDentity Applet Suite v4.0 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after several configuration steps it

[1] The applet is provided in cap file format.
[2] The AGD documents provided in electronic document format.

will be personalized as IDentity Applet v4.0/BAC. For details please see: section 1.4.4 TOE life cycle and [5].

The boxes marked with white are not certified.

1.4.3. TOE usage and security features for operational use

A State or Organisation 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

(iv) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and
(v) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

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

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [13]. These security measures can include the binding of the travel document's chip to the travel document.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, 'ICAO Doc 9303' [13].

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 does not address the Extended Access Control as optional security mechanisms.

The TOE support the Active Authentication (defined by [13]) as an optional security mechanism The Active Authentication enables to the inspection system to verify that the TOE chip is genuine, based on a static key pair (Active Authentication Key Pair) stored in the chip.

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

(iii) Reads optically the MRTD,
(iv) authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system according to [13].

1.4.4. TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [15], the TOE life cycle the life-cycle is additionally subdivided into 7 steps.)

Application note 3 (from ST Author)

The IDentity Applet Life cycle has the following phases, which differ from the whole TOE Life cycle:

- IDentity Applet

LOADED (Creation phase)

- IDentity Instance

Personalization Phase

SELECTABLE (Configuration Phase)

CONFIGURED (Initialization Phase)

Operational Phase

PERSONALIZED

LOCKED

BLOCKED

These phases are detailed in the ID&Trust IDentity Applet Suite Administrator's Guide [5]. These states and phases are presented here, because of informational reasons, to serve better understanding.

Phase 1 of TOE life-cycle "Development"

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

(Step2) IC developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system). The IDentity Applet v4.0/BAC and the corresponding guidance documentation are developed by ID&Trust Ltd.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software and the IDentity Applet v4.0/BAC in the non-volatile non-programmable memories and in FLASH

is securely delivered to the IC manufacturer. Part of the IC Embedded Software is in the non-volatile non-programmable memories, and the guidance documentation is securely delivered to the travel document manufacturer.

Application note 4 (from ST author)

The delivery procedures between ID&Trust (applet developer) and the manufacturer:

1. The IDentity Applet Developer develops a new version of the ID&Trust IDentity Applet v4.0/BAC.
2. After the new version is tested a new release is issued and stored in configuration management system.
3. The new version of the IDentity Applet v4.0 is sent to as required by [27].

Phase 2 of TOE life cycle "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (ROM) and the IDentity Applet Suite v4.0 uploaded to FLASH. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacture to the travel document manufacturer.

Application note 5 (from ST author):

The IC (wafer) is placed into the inlay by the inlay provider (in the case of a contact interface, implantation is performed) and is then forwarded in this form to the travel document manufacturer. Throughout the process, the TOE remains in a protected state.

(Step4) The NXP (i) load the IDentity Applet and (ii) equips MRTD's chips with pre-personalization data.

Application note 6 (redefined for the goals of this ST by the ST author, taken from Application note 1 from [17]):

Creation of the application involves that the Creation Phase of the IDentity Applet is closed, and the IDentity Applet gets to SELECTABLE state (Configuration Phase). Further details are discussed within the IDentity Applet Administrator's Guide [5]. This process is managed by the Personalisation agent.

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

The Personalization Agent Authentication Keys are the preinstalled keys for the IDentity Applet, which are preinstalled by the Travel Document Manufacturer, and which are needed and used in the Personalization process.

Phase 3 of TOE life-cycle "Personalisation of the travel document"

(Step5) The personalisation of the travel document includes:

I. the survey of the travel document holder's biographical data,
II. the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
III. the printing of the visual readable data onto the physical part of the travel document,

IV. the writing of the TOE User Data and TSF Data into the logical travel document and
V. configuration of the TSF if necessary.

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

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

Application note 7 (of the ST author)

The Personalisation Phase of the IDentity Applet contains the Configuration and Initialisation Phase.

During Configuration phase all applications, files, security data objects, configuration variables, file and object parameters are created. Specified settings in the configuration phase fundamentally determine the Application Profile, which is protected by the Application Profile Signature.

In the Initialisation Phase the content of the IDentity Applet instance is loaded. The signing of the Document Security Object by the Document Signer is crucial in this phase since the signature of the Document Security Object supports to verify genuineness of the MRTD's chip (DG.15 with Active Authentication).

The referred Personalization Agent can be the Card Issuer, or a different contributor on the Card Issuer discretion.

These phases are detailed in the ID&Trust IDentity Applet Suite Administrator's Guide [5]. These states and phases are presented here for informational reasons, to serve better understanding.

Application note 8 (taken from application note 2 from [17])

The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Phase 4 of the TOE life-cycle "Operational Use"

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

Application note 9 (taken from application note 4 from [17]))

The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 "Operational Use". This will imply an update of the Document Security Object including the re-signing by the Document Signer.

Application note 10 (taken from application note 5 from [17])

The intention of the ST is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless, the decision about this has

to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalisation process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

1.4.5. TOE security functions

The following TOE ensured security functions are the most significant for its operational use:

- Only entities (e.g. terminals) possessing authorisation can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the entity connected,
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

Above mentioned functions are described below informally, and in detail in section 7.1.

1.4.6. Features of the IDentity Applet

This section is informational and intended to provide a general detail about the IDentity Applet which is the essential part of this ST. Information in this section does not extend the TOE description or claims of this ST.

IDentity Applet may be considered as a highly secure and configurable multi-application cryptographic smart card framework for PKI and e-ID purposes.

IDentity Applet complies with the standards referenced in TOE Overview.

The API exposed by IDentity Applet allows fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and Payment applications.

IDentity is designed for the Java Card family of smart card platforms and specifically for the NXP JCOP IC which is certified according to the CC EAL 6+ both the microprocessor and the JCOP OS as well. Platform is protected against state of the art attacks.

The Platform provides:

- Cryptographic algorithms and functionality (3DES, AES, RSA, SHA, ECDSA, RNG, DH, ECDH, etc.);
- GlobalPlatform 2.3 functionality;
- Three different communication protocol (ISO 7816 T=0, T=1, ISO 14443 T=CL (contact-less);
- Java Card 3.0.5 functionality (secure memory management, garbage collection, extended Length APDUs, etc.)

- NXP Proprietary functionality (Secure Box, Secure Messaging Accelerator Interface, JAVA CARD API for data encryption via PUF).

2. Conformance Claims

2.1. CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017[2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [3]

as follows

- Part 2 extended, (see Chapter 5 Extended components definition)
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]

has to be taken into account.

2.2. PP Claim

The current ST claims strict conformance to the following Protection Profile:

Title:	Protection Profile — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP) [17]
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1 (Revision 2)
Assurance Level:	The minimum assurance level for this PP is EAL4 augmented.
General Status:	Final
Version Number:	1.10
Registration:	BSI-CC-PP-0055
Keywords:	ICAO, machine readable travel document, basic access control

2.3. Package Claim

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 [3].

2.4. Conformance rationale

The security target claims strict conformance to one PP ([17]).

This ST is conformant with Common Criteria Part 2 [2] extended due to additional components as stated in Protection Profile named above in the PP claim.

This ST is conformant to Common Criteria Part 3 [3]

The TOE is consistent with the TOE type in the PP.

The security problem definition of this security target is consistent with the statement of the security problem definition in the PP, as the security target claims strict conformance to the PP.

All assignments and selections of the security functional requirements defined in the [17] are done accordingly.

There is one assumption is refined:

A.Insp_Sys

Justification is modified because of the optional function of the TOE (Active Authentication).

This refined A.Insp_Sys assumption does not affect the strict conformance.

There is one threat added:

- T.Counterfeit.

Justification: T.Counterfeit is added because of the optional function of the TOE (Active Authentication).

This threat does not affect the strict conformance.

The security objectives for the TOE of this security target are consistent with the statement of the security objectives in the PP as the security target claims strict conformance to the PP. There is one security objective added:

- OT.Active_Auth_Proof (Proof of travel document's chip authenticity).

Justification: OT.Active_Auth_Proof is added because of the optional function of the TOE (Active Authentication).

This security objective does not affect the strict conformance.

The security objectives for the operational environment in this security target include all security objectives for the operational environment from the PP. There are one objectives added:

- OE.Active_Auth_Key_Travel_Document (Travel document Active Authentication Key).

Justification: OE.Active_Auth_Key_Travel_Document is added because of the optional function of the TOE (Active Authentication).

This security objectives do not affect the strict conformance.

The security requirements of this ST are consistent with the statement of the security requirements in the [17] as the ST claims strict conformance to the [17]. There is the following SFRs added from sec. 6.1 in this security target: FIA_API.1/AA, The following SFRs were iterated from [2]:

- FCS_CKM.1/AA_GEN
- FMT_MTD.1/AAPK
- FCS_COP.1/EMRTD.

Two existing SFRs were extended for the inclusion of the Active Authentication private key:

- FMT_MTD.1/KEY_READ, and
- FPT_EMS.1.

Justification: The above-mentioned addition, iterations and extensions are necessary because of the optional function of the TOE (Active Authentication).

These additional SFRs do not affect the strict conformance. All assignments and selections of the security functional requirements are defined in the [17] section 6.1 and in this security target section 6.1.

2.5. Statement of compatibility

2.5.1. Security Functionalities

The following table contains the security functionalities of the Platform-ST [7] and of this ST, showing which Functionality correspond to the Platform-ST [7] and which has no correspondence. This statement is compliant to the requirements of [8].

A classification of TSFs of the Platform-ST [7] has been made. Each TSF has been classified as 'relevant' or 'not relevant' for this ST.

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant/ Not relevant	Remarks
SF.JCVM	TSF.Platform	Relevant	Java Card Virtual Machine
SF.CONFIG	TSF.Platform TSF.CryptoKey	Relevant	Configuration Management
SF.OPEN	TSF.Authenticate TSF.SecureManagement TSF.Platform	Relevant	Card Content Management
SF.CRYPTO	TSF.CryptoKey TSF.AppletParametersSign TSF.Platform	Relevant	Cryptographic Functionality
SF.RNG	TSF.CryptoKey TSF.Platform	Relevant	Random Number Generator
SF.DATA_STORAGE	TSF.CryptoKey TSF.AppletParametersSign TSF.Platform	Relevant	Secure Data Storage
SF.PUF	-	Not relevant	User Data Protection using PUF
SF.OM	TSF.Platform	Relevant	Java Object Management
SF.MM	TSF.CryptoKey TSF.Platform	Relevant	Memory Management
SF.PIN	-	Not relevant	PIN Management
SF.BIO	-	Not relevant	Biometric Template Management
SF.PERS_MEM	TSF.Platform	Relevant	Persistent Memory Management

SF.EDC	TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.PID	TSF.Platform	Relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	-	Module Invocation
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.OSU	-	Not relevant	OS Update
SF.MOD_DEL	-	Not relevant	Module Deletion

Table 2 Classification of Platform-TSFs

All the above Platform TSFs which are indicated as relevant are relevant for this ST.

Application note 11 (by the ST author)

The TSF.Platform Security functionality in the above list represents functionalities which are not directly used in the IDentity Applet v4.0/BAC, they are implicitly invoked by calls to the Platform, respectively the operating system. These functions are called altogether as TSF.Platform.

2.5.2. OSPs

The P.Manufact of this ST is relevant but is covered by the Platform's certification.

None of the other OSPs of this ST are applicable to the Platform and therefore not mappable for the Platform-ST.

The OSPs from the Platform-ST [7] OSP.VERIFICATION, OSP.KEY-CHANGE, OSP.SECURITY-DOMAINS, OSP.SECURE-BOX does not deal with any additional security components.

2.5.3. Security objectives

These Platform-ST [7] objectives can be mapped to this STs objectives as shown in the following table, so they are relevant.

Objectives form the Platform ST	Objectives form this ST
OT.ALARM	OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper
OT.APPLI-AUTH	OT.AC_Pers OT.Data_Int OT.Data_Conf OT.Active_Auth_Proof
OT.CARD-CONFIGURATION	OT.Prot_Abuse-Func OT.Prot_Inf_Leak
OT.CARD-MANAGEMENT	OT.Data_Conf OT.Identification OT.Data_Conf OT.Data_Int

	OT.Prot_Abuse-Func
OT.CHIPHER	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Active_Auth_Proof
OT.COMM_AUTH	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Active_Auth_Proof OT.Prot_Abuse-Func OT.Identification
OT.COMM_CONFIDENTIALITY	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Prot_Abuse-Func OT.Identification OT.Active_Auth_Proof
OT.COMM_INTEGRITY	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Prot_Abuse-Func OT.Identification OT.Active_Auth_Proof
OT.DOMAIN-RIGHTS	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Prot_Abuse-Func OT.Identification
OT.FIREWALL	OT.AC_Pers OT.Data_Conf OT.Data_Int
OT.GLOBAL_ARRAYS_CONFID	OT.AC_Pers OT.Data_Conf
OT.TOE_IDENTIFICATION	OT.Identification
OT.KEY-MNGT	OT.AC_Pers OT.Data_Conf OT.Data_Int OT.Active_Auth_Proof
OT.OBJ-DELETION	OT.Prot_Abuse-Func OT.Prot_Inf_Leak
OT.OPERATE	OT.AC_Pers OT.Prot_Abuse-Func OT.Prot_Inf_Leak
OT.REALLOCATION	OT.AC_Pers OT.Data_Conf
OT.RESOURCES	OT.AC_Pers OT.Data_Conf

	OT.Data_Int OT.Prot_Abuse-Func OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.RND	OT.AC_Pers OT.Data_Conf OT.Data_Int
OT.SCP.IC	OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.SCP.RECOVERY	OT.Prot_Inf_Leak OT.Prot_Malfunction
OT.SCP.SUPPORT	OT.AC_Pers OT.Data_Int OT.Data_Conf OT.Active_Auth_Proof
OT.SENSITIVE_RESULTS_INTEG	OT.Prot_Inf_Leak
OT.SID	OT.AC_Pers OT.Data_Int OT.Data_Conf
OT.TRANSACTION	OT.AC_Pers OT.Data_Conf

Table 3 Mapping of security objectives for the TOE

The following Platform-ST [7] objectives are not relevant for or cannot be mapped to the TOE of this ST:

- OT.AUTH-LOAD-UPDATE-IMAGE
- OT.BIO-MNGT
- OT.GLOBAL_ARRAYS_INTEG
- OT.CONFID-UPDATE-IMAGE.LOAD
- OT.NATIVE
- OT.PIN-MNGT (There is no PIN management in the TOE.)
- OT.SEC_BOX_FW
- OT.SECURE_ACTIVATION_ADDITIONAL_CODE
- OT.SECURE_LOAD_ACODE
- OT.SID_MODULE

The objectives for the operational environment can be mapped as follows:

Security Objectives for the environment of the Platform-ST	Classification of OE	Comments
OE.APPLET	CfPOE	Covered by ALC class
OE.APPS-PROVIDER	CfPOE	Covered by ALC class
OE.CODE-EVIDENCE	CfPOE	Covered by ALC class
OE.CONFID-UPDATE-IMAGE.CREATE	CfPOE	Covered by ALC class
OE.KEY-CHANGE	CfPOE	Covered by ALC class

OE.PROCESS_SEC_IC	CfPOE	Covered by the Platform's certification and ALC class
OE.SECURITY-DOMAINS	CfPOE	Covered by ALC class
OE.USE_DIAG	SgOE	Covered by OE.Exam_MRTD and OE.Prot_Logical_MRTD
OE.USE_KEYS	SgOE	Covered by OE.Exam_MRTD and OE.Prot_Logical_MRTD
OE.VERIFICATION	CfPOE	Covered by ALC class
OE.VERIFICATION-AUTHORITY	CfPOE	Covered by ALC class

Table 4 Mapping of security objectives of the environment

There is no conflict between security objectives of this ST and the Platform-ST.

2.5.4. Security requirements

The Security Requirements of the Platform-ST [7] can be mapped as follows:

Platform SFR	Composite TOE SFRs	Category of Platform's SFR	Remarks
FAU_ARP.1	FPT_PHP.3	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by FPT_PHP.3.
FAU_SAS.1[SCP]	FAU_SAS.1	RP_SFR-MECH	FAU_SAS.1[SCP] covers the requirement of FAU_SAS.1.
FCO_NRO.2[SC]	-	IP_SFR	Not relevant
FCS_CKM.1	FCS_CKM.1/AA_GEN	RP_SFR-SERV	FCS_CKM.1 applied to generate the Active Authentication key pair on the TOE.
FCS_CKM.2	-	IP_SFR	-
FCS_CKM.3	-	IP_SFR	-
FCS_CKM.4	-	IP_SFR	-
FCS_COP.1	FCS_CKM.1	RP_SFR-SERV	The FCS_COP.1[SHA] applied during the key derivation function in FCS_CKM.1.
	FCS_COP.1/SHA	RP_SFR-SERV	The FCS_COP.1[SHA] applied during hash generation in FCS_COP.1/SHA
	FCS_COP.1/ENC	RP_SFR-SERV	The FCS_COP.1[TripleDES] applied during encryption and decryption in FCS_COP.1/ENC
	FCS_COP.1/MAC	RP_SFR-SERV	The FCS_COP.1[DESMAC] applied during message authentication code generation and verification in FCS_COP.1/MAC
	FCS_COP.1/EMRTD	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] applied during digital signature generation in FCS_COP.1/EMRTD

Platform SFR	Composite TOE SFRs	Category of Platform's SFR	Remarks
	FCS_COP.1/AUTH	RP_SFR-SERV	FCS_COP.1.1[TripleDES] applied for encryption and decryption in FCS_COP.1/AUTH.
	FIA_UAU.6	RP_SFR-SERV	FCS_COP.1.1[DESMAC] is applied for MAC calculation.
	FIA_API.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] applied during digital signature generation related to Active Authentication.
	FDP_UCT.1	RP_SFR-SERV	The FCS_COP.1[TripleDES] applied during secure messaging to protect user data from unauthorized disclosure.
	FDP_UIT.1	RP_SFR-SERV	The FCS_COP.1[DESMAC] applied during message messaging to protect again modification, deletion, insertion and replay errors
FCS_RNG.1	FCS_CKM.1	RP_SFR-SERV	FCS_RNG.1 applied for secure random generation in FCS_CKM.1.
	FCS_RND.1	RP_SFR-SERV	FCS_RNG.1 applied for secure random in FCS_RND.1.
	FIA_UAU.4	RP_SFR-SERV	FCS_RNG.1 applied for generating fresh nonce for FIA_UAU.4.
FCS_RNG.1[HDT]	-	IP_SFR	Not relevant
FDP_ACC.1[SD]	-	IP_SFR	Not relevant
FDP_ACC.2[FIREWALL]	-	IP_SFR	Not relevant
FDP_ACC.2[ADEL]	-	IP_SFR	Not relevant
FDP_ACC.2[SecureBox]	-	IP_SFR	Not relevant
FDP_ACF.1[ADEL]	-	IP_SFR	Not relevant
FDP_ACF.1[SecureBox]	-	IP_SFR	Not relevant
FDP_ACF.1[FIREWALL]	-	IP_SFR	Not relevant
FDP_ACF.1[SD]	-	IP_SFR	Not relevant
FDP_IFC.1[JCVM]	-	IP_SFR	Not relevant
FDP_IFC.2[SC]	FIA_UAU.5	RP_SFR-MECH	Authentication based on GP keys is handled by FDP_IFC.2[SC]
FDP_IFC.2[CFG]	FMT_LIM.1 FMT_LIM.2	RP_SFR-MECH	FDP_IFC.2[CFG] applied for to protect the TOE in operational phase.
FDP_IFC.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant

Platform SFR	Composite TOE SFRs	Category of Platform's SFR	Remarks
FDP_IFF.1[JCVM]	-	IP_SFR	Not relevant
FDP_IFF.1[SC]	FMT_MTD.1/INI_ENA FMT_MTD.1/INI_DIS	RP_SFR-MECH	FDP_IFF.1[SC] applied to control the writing of initialization and pre-personalization data as required by FMT_MTD.1/INI_ENA, and FMT_MTD.1/INI_DIS
FDP_IFF.1[CFG]	-	IP_SFR	Not relevant
FDP_IFF.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FDP_ITC.2[CCM]	-	IP_SFR	Not relevant
FDP_RIP.1[OBJECTS]	-	IP_SFR	Not relevant
FDP_RIP.1[ABORT]	-	IP_SFR	Not relevant
FDP_RIP.1[APDU]	-	IP_SFR	Not relevant
FDP_RIP.1[bArray]	-	IP_SFR	Not relevant
FDP_RIP.1[GlobalArray_Refined]	-	IP_SFR	Not relevant
FDP_RIP.1[KEYS]	-	IP_SFR	Not relevant
FDP_RIP.1[TRANSIENT]	FCS_CKM.4	RP_SFR-MECH	FDP_RIP.1[TRANSIENT] is responsible to destroy the session keys.
FDP_RIP.1[ADEL]	-	IP_SFR	Not relevant
FDP_RIP.1[ODEL]	-	IP_SFR	Not relevant
FDP_ROL.1[FIREWALL]	-	IP_SFR	Not relevant
FDP_ROL.1[CCM]	-	IP_SFR	Not relevant
FDP_SDI.2[DATA]	FPT_TST.1	RP_SFR-MECH	FDP_SDI.2[DATA] checks the integrity of specific user data.
FDP_SDI.2[SENSITIVE_RESULT]	FPT_TST.1	RP_SFR-MECH	FDP_SDI.2[SENSITIVE_RESULT] checks the integrity error related to sensitive API result.
FDP_UIT.1[CCM]	-	IP_SFR	Not relevant
FIA_AFL.1[BIO]	-	IP_SFR	Not relevant
FIA_AFL.1[PIN]	-	IP_SFR	Not relevant
FIA_ATD.1[AID]	-	IP_SFR	Not relevant
FIA_ATD.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FIA_UID.1[SC]	FIA_UID.1	RP_SFR-MECH	The FIA_UID.1[SC] handles the identifier data of the TOE.
FIA_UID.1[CFG]	-	IP_SFR	Not relevant
FIA_UID.2[AID]	-	IP_SFR	Not relevant
FIA_UID.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FIA_USB.1[AID]	-	IP_SFR	Not relevant
FIA_USB.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FIA_UAU.1[SC]	FIA_UAU.1	RP_SFR-MECH	The FIA_UAU.1[SC] handles the identifier data of the TOE.

Platform SFR	Composite TOE SFRs	Category of Platform's SFR	Remarks
FIA_UAU.4[SC]	-	IP_SFR	Not relevant
FMT_MSA.1[JCRE]	-	IP_SFR	Not relevant
FMT_MSA.1[JCVM]	-	IP_SFR	Not relevant
FMT_MSA.1[ADEL]	-	IP_SFR	Not relevant
FMT_MSA.1[SC]	-	IP_SFR	Not relevant
FMT_MSA.1[SecureBox]	-	IP_SFR	Not relevant
FMT_MSA.1[CFG]	-	IP_SFR	Not relevant
FMT_MSA.1[SD]	-	IP_SFR	Not relevant
FMT_MSA.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FMT_MSA.2[FIREWALL-JCVM]	-	IP_SFR	Not relevant
FMT_MSA.3[FIREWALL]	-	IP_SFR	Not relevant
FMT_MSA.3[JCVM]	-	IP_SFR	Not relevant
FMT_MSA.3[ADEL]	-	IP_SFR	Not relevant
FMT_MSA.3[SecureBox]	-	IP_SFR	Not relevant
FMT_MSA.3[CFG]	-	IP_SFR	Not relevant
FMT_MSA.3[SD]	-	IP_SFR	Not relevant
FMT_MSA.3[SC]	-	IP_SFR	Not relevant
FMT_MSA.3[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FMT_MTD.1[JCRE]	-	IP_SFR	Not relevant
FMT_MTD.3[JCRE]	-	IP_SFR	Not relevant
FMT_SMF.1	-	IP_SFR	Not relevant
FMT_SMF.1[ADEL]	-	IP_SFR	Not relevant
FMT_SMF.1[SecureBox]	-	IP_SFR	Not relevant
FMT_SMF.1[CFG]	-	IP_SFR	Not relevant
FMT_SMF.1[SD]	-	IP_SFR	Not relevant
FMT_SMF.1[SC]	FMT_SMF.1	RP_SFR-MECH	FMT_SMF.1[SC] partly covers the functions FMT_SMF.1 (GlobalPlatform).
FMT_SMF.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FMT_SMR.1	-	IP_SFR	Not relevant
FMT_SMR.1[INSTALLER]	-	IP_SFR	Not relevant
FMT_SMR.1[ADEL]	-	IP_SFR	Not relevant
FMT_SMR.1[CFG]	-	IP_SFR	Not relevant
FMT_SMR.1[SD]	-	IP_SFR	Not relevant
FMT_SMR.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FPR_UNO.1	-	IP_SFR	Not relevant
FPT_EMSEC.1	FPT_EMS.1	RP_SFR-MECH	FPT_EMS.1 matches the FPT_EMSEC.1 of the Platform.

Platform SFR	Composite TOE SFRs	Category of Platform's SFR	Remarks
FPT_FLS.1	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1 of the Platform ensures the secure state of the TOE as required by FPT_FLS.1
FPT_FLS.1[INSTALLER]	-	IP_SFR	Not relevant
FPT_FLS.1[ADEL]	-	IP_SFR	Not relevant
FPT_FLS.1[ODEL]	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1[ODEL] of the Platform ensures the secure state of the TOE as required by FPT_FLS.1
FPT_FLS.1[CCM]	-	IP_SFR	Not relevant
FPT_FLS.1[MODULAR-DESIGN]	-	IP_SFR	Not relevant
FPT_TDC.1	-	IP_SFR	Not relevant
FPT_RCV.3[INSTALLER]	-	IP_SFR	Not relevant
FPT_PHP.3	FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3 matches the FPT_PHP.3 of the Platform.
FTP_ITC.1[SC]	-	IP_SFR	Not relevant
ADV_SPM.1	-	IP_SFR	Not relevant
FDP_IFC.2[OSU]	-	IP_SFR	-
FDP_IFC.2[OSU]	-	IP_SFR	-
FDP_IFC.2[OSU]	-	IP_SFR	-
FDP_IFF.1[OSU]	-	IP_SFR	-
FIA_UAU.1[OSU]	-	IP_SFR	-
FIA_UAU.4[OSU]	-	IP_SFR	-
FIA_UID.1[OSU]	-	IP_SFR	-
FMT_MSA.1[OSU]	-	IP_SFR	-
FMT_MSA.1[OSU]	-	IP_SFR	-
FMT_MSA.3[OSU]	-	IP_SFR	-
FMT_MSA.3[OSU]	-	IP_SFR	-
FMT_SMF.1[OSU]	-	IP_SFR	-
FMT_SMF.1[OSU]	-	IP_SFR	-
FMT_SMR.1[OSU]	-	IP_SFR	-
FMT_SMR.1[OSU]	-	IP_SFR	-
FMT_SMR.1[OSU]	-	IP_SFR	-
FPT_FLS.1[OSU]	-	IP_SFR	-
FDP_ACC.2[MDEL]	-	IP_SFR	-
FDP_ACF.1[MDEL]	-	IP_SFR	-
FDP_RIP.1[MDEL]	-	IP_SFR	-
FMT_MSA.1[MDEL]	-	IP_SFR	-
FMT_MSA.3[MDEL]	-	IP_SFR	-
FMT_SMF.1[MDEL]	-	IP_SFR	-
FMT_SMR.1[MDEL]	-	IP_SFR	-
FPT_FLS.1[MDEL]	-	IP_SFR	-

Table 5 Mapping of Security requirements

The FMT_LIM.1 and FMT_LIM.2 are just partly covered directly by [7]. As described in [17] the purpose of these SFRs is to prevent misuse of test features of the TOE over the life cycle phases.

According to [7] the Platform consists of the Micro Controller, Crypto Library and Operation System, which are certified as well. By the Micro Controller the limited availability and capability of test features are ensured after Manufacturing phase of the TOE. FMT_LIM.1 and FMT_LIM.2 are covered by the following Security Function of Micro Controller ST: TSF.Control. For details, please check[32].

To sum up the above-mentioned Security Function of Micro Controller ensures that the test features of TOE cannot be misused.

The Personalization Agent (FMT_SMR.1) may use the GlobalPlatform function of the Platform.

2.5.5. Assurance requirements

This ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by ALC_DVS.2.

The Platform-ST [7] requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ASE_TSS.2 and ALC_FLR.1.

As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the Platform-ST [7] assurance requirements.

2.6. Analysis

Overall, there is no conflict between security requirements of this ST and the Platform-ST [7].

3. Security Problem Definition

3.1. Assets

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

Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [13]. 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. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the 'ICAO Doc 9303' [13] the TOE described in this security target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

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

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

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

3.2. Subjects

This security target considers the following subjects:

Manufacturer

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 user's IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

The Manufacturer of the chip is the NXP company. The ID&Trust IDentity Applet Suite v4.0 is located on the card.

Personalization Agent

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
(v) signing the Document Security Object defined in [13].

Currently Application Profile Provider is ID&Trust.

Terminal

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

Inspection system (IS)

A technical system used by the border control officer of the receiving State

(i) examining an MRTD presented by the traveler and verifying its authenticity and
(i) 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.

Application note 12 (modified by ST author, taken from application note 6 from [17])

This security target does not distinguish between the BIS, GIS and EIS because the Extended Access Control is outside the scope. All terminals may be able to support Active Authentication protocol.

MRTD Holder

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

Traveler

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

Attacker

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 13 (taken from application note 7 from [17])

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.

3.3. Assumptions

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

A.MRTD_Manufact

MRTD manufacturing on steps 4 to 6

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

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.

Application note 14 (of the ST Author)

The delivery procedures between ID&Trust (applet developer) and the manufacturer:

1. The IDentity Applet Developer develops a new version of the ID&Trust IDentity Applet v4.0/BAC.
2. After the new version is tested a new release is issued and stored in configuration management system.
3. The new version of the IDentity Applet v4.0 is sent to as required by [27].

A.Pers_Agent

Personalization of the MRTD's chip

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.

PERSONALIZED state of the IDentity Applet v4.0/BAC indicates that the IDentity Applet v4.0/BAC is in the Operational Phase. In this phase the corresponding standard [13] and documented behaviour is followed. In Operational phase access control for eID functions and data objects are activated and managed according to the pre-defined security attributes and security environments.

A.Insp_Sys
Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State:

(i) examining an MRTD presented by the traveller and verifying its authenticity and
(ii) verifying the traveller 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 [13].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

The Basic Inspection System may support the Active Authentication, in this case the Basic Inspection System implements the terminal part of Active Authentication (defined in [13]).

Application note 15 (taken from application note 8 from [17])

According to [13] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

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

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [13], 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.

Application note 16 (taken from application note 9 from [17])

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.

3.4. Threats

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

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

T.Chip_ID

Identification of MRTD's chip

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

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

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

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

The TOE shall avert the threats as specified below.

T.Abuse-Func
Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order

(i) to manipulate User Data,
(ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
(iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to 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

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

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

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

T.Counterfeit

Counterfeit of travel document chip data

Adverse action: An attacker with enhanced-basic attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document

The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

Threat agent: having enhanced-basic attack potential, being possession of one or more legitimate travel documents

Asset: authenticity of logical MRTD

3.5. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. A.6).

P.Manufact

Manufacturing of the MRTD's chip

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

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

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) 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 [13].

Application note 17 (taken from application note 10 from [17])

The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [13]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4. Security Objectives

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

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.

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 [13] 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.

Application note 18 (taken from application note 11 from [17])

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) cannot be changed by write access after personalization,
(2) the Personalization Agents may
    (a) add (fill) data into the LDS data groups not written yet, and
    (b) update and sign the Document Security Object accordingly.

The support for adding data in the “Operational Use” phase is optional.

OT.Data_Int

Integrity of personal data

The TOE must ensure the integrity of the logical 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.

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.

Application note 19 (taken from application note 12 from [17])

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' [13] 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.

OT.Identification

Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the 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.

Application note 20 (taken from application note 13 from [17])

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.

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

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 IC Embedded 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.

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

(i) 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
(ii) by forcing a malfunction of the TOE and/or
(iii) by a physical manipulation of the TOE.

Application note 21 (taken from application note 14 from [17])

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper

Protection against Physical Tampering

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

(i) 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
(ii) 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)
(iii) manipulation of the hardware and its security features, as well as
(iv) controlled manipulation of memory contents (User Data, TSF Data)

with a prior

(v) reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction

Protection against Malfunctions

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

Application note 22 (taken from application note 15 from [17])

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

The following Security Objective for the TOE is defined in addition to the objectives given by the [17] to cover the Active Authentication mechanism.

OT.Active_Auth_Proof
Proof of travel document's chip authenticity

The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Active Authentication as defined in [13]. The authenticity proof provided by travel document's chip shall be protected against attacks with enhanced-basic attack potential.

4.2. Security Objectives for the Operational Environment

4.2.1. Issuing State or Organization

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

OE.MRTD_Manufact
Protection of the MRTD Manufacturing

Appropriate functionality testing of the TOE shall be used in step 4 to 5.

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

OE.MRTD_Delivery
Protection of the MRTD delivery

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

i. non-disclosure of any security relevant information,
ii. identification of the element under delivery,
iii. meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
iv. physical protection to prevent external damage,
v. secure storage and handling procedures (including rejected TOE's),
vi. traceability of TOE during delivery including the following parameters:
    a. origin and shipment details,
    b. reception, reception acknowledgement,
    c. location material/information.

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

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

OE.Personalization

Personalization of logical 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.

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 [13].

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' [13] 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.

4.2.2. Receiving State or Organization

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

OE.Exam_MRTD

Examination of the 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 [13].

OE.Passive_Auth_Verify

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.

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).

OE.Active_Auth_Key_Travel_Document

Travel document Active Authentication Key

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

i. generate the travel document's Active Authentication Key Pair if necessary,
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 proof the authenticity of the active authentication public key by Passive Authentication.

4.3. Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verify	OE.Prot_Logical_MRTD	OE.Active_Auth_Key_Travel_Document
T.Chip_ID	-	-	-	x	-	-	-	-	-	-	-	-	-	x	-	-	-	-
T.Skimming	-	-	x	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-
T.Eavesdropping	-	-	x	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-
T.Forgery	x	x	-	-	-	-	x	-	-	-	-	-	x	-	x	x	-	-
T.Counterfeit	-	-	-	-	-	-	-	-	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	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
A.MRTD_Manufact	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-
A.MRTD_Delivery	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-
A.Pers_Agent	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-
A.Insp_Sys	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	x	X
A.BAC-Keys	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-

Table 6 Security Objective Rationale

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.

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.

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 Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the

security objectives OT.Data_Int “Integrity of personal data” describing the unconditional protection of the integrity of the stored data and during transmission. The security objective OT.Data_Conf “Confidentiality of personal data” describes the protection of the confidentiality.

The threat T.Chip_ID “Identification of 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.

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.

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”.

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.

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 enhanced-basic attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives OT.Prot_Inf_Leak “Protection against Information Leakage”, OT.Prot_Phys-Tamper “Protection against Physical Tampering” and OT.Prot_Malfunction “Protection against Malfunctions”.

The threat T.Counterfeit “Counterfeit of travel document’s chip data” is thwarted through the chip by an identification and authenticity proof required by OT.Active_Auth_Proof “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing state or organisation. The

Active Authentication public key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by OE.Active_Auth_Key_Travel_Document “Travel Document Active Authentication Key”.

The assumption A.MRTD_Manufact “MRTD manufacturing on step 4 to 5” 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 5” 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.

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.

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. OE.Active_Auth_Key_Travel_Document (Travel document Active Authentication Key) will require the Basic Inspection System to implement the Active Authentication protocol.

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

5. Extended Components Definition

This security target uses components defined as extensions to [2], which are defined in the relevant PP-0055 [17] protection profile. The FIA_API family taken from [18] because of the optional functionality of the TOE (Active Authentication).

5.1. Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

Family behavior:

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling

FAU_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management:	FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies

FIA_API.1.1The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

5.2. Definition of the Family FAU_SAS

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

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

FAU_SAS Audit data storage

Family behavior:

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

Component levelling

FAU_SAS Audit data storage	1

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies

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

5.3. Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1.

The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family "Generation of random numbers (FCS_RND)" is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:

FCS_RND Generation of random numberts	1

FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	Quality metric for random numbers
Hierarchical to:	No other components.
Dependencies:	No dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

5.4. Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts 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.
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 lifecycle.

Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

FMT_LIM.1	**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].

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

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

Application note 23 (taken from application note 16 from [17])

The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the 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 test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

5.5. Definition of the Family FPT_EMS

Application note 24 (from ST author)

The [17] use the FPT_EMSEC, but according to [2] 7.1.2.1: "The categorical information consists of a short name of seven characters, with the first three identical to the short name of the class followed by an underscore and the short name of the family as follows XXX_YYY." In order to fulfil the referenced CC requirement, in current ST FPT_EMS will be applied. The content of the FPT_EMSEC is not modified.

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

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

FMT_EMS TOE emanation

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS TOE emanation	1

FPT_EMS.1	TOE emanation has two constituents:
FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMS.1
	There are no management activities foreseen.
Audit:	FPT_EMS.1
	There are no actions defined to be auditable.
FPT_EMS.1	**TOE Emanation**

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

6. Security Requirements

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

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

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. 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 are italicized. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

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 like this. Assignments filled in by the ST author are denoted as double underlined text.

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

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Basic Inspection System” and “Terminal” used in the following chapter is given in section 3.2. 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 [2].

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 successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

Table 7 Definition of security attributes

The following objects are defined in addition to the objects to cover the Active Authentication mechanism:

Name	Data
Active Authentication Key Pair	The Active Authentication Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication mechanism according to [13].
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment. A hash representation of DG15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SOD).
Active Authentication Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Table 8 Additionally defined objects for Active Authentication

6.1. Security Functional Requirements for the TOE

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

6.1.1. Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1
Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1

The TSF shall provide the Manufacturer[3] with the capability to store the IC Identification Data[4] in the audit records.

Application note 25 (taken from application note 17 from [17])

The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or

[3] [assignment: *authorised users*]
[4] [assignment: *list of audit information*]

Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2. Class Cryptographic Support (FCS)

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

FCS_CKM.1
Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[5] and specified cryptographic key sizes 112 bit[6] that meet the following: [13][7].

Application note 26 (redefined by ST author, taken from application note 18 from [17])

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 [13] part 11 4.3, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [13] part 11 informative appendix D. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

FCS_CKM.1/AA_GEN
Cryptographic key generation – Active Authentication key

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_COP.1/EMRTD. FCS_CKM.4 Cryptographic key destruction: not fulfilled but justified. Justification: The Active Authentication key pair cannot be deleted or regenerated.

FCS_CKM.1.1/AA_GEN

[5] [assignment: *cryptographic key generation algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECC and RSA[8] and specified cryptographic key sizes ECC 160, 192, 224, 256, 384, 512, 521bits and RSA 1024, 1280, 1536, 1984, 2048, 4096 bit[9] that meet the following:[13][10].

Application note 27 (from the ST author)

The Active Authentication key pair can either be generated in the TOE or imported by the Personalisation Agent (cf. FMT_MTD.1/AAPK). This SFR has been included in this security target in addition to the SFRs defined by the [17] claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed [17].

Application note 28 (from the ST author)

The underlying Platform supports RSA and ECDSA signature algorithms and cryptographic key length 1024 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA). These key lengths are supported with equivalent implementation-level security measures. However, to defend against attackers with high attack potential, the actual key length chosen for use during the operational phase must be appropriate and in line with current cryptographic recommendations. When selecting the key length, consideration must be given to the expected lifetime of the TOE to ensure that the chosen cryptographic strength remains sufficient throughout the entire operational lifespan.

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

FCS_CKM.4
Cryptographic key destruction - MRTD

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 deallocation of the resource[11] that meets the following: none[12].

Application note 29 (taken from application note 19 from [17])

The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

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

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

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA

The TSF shall perform hashing[13] in accordance with a specified cryptographic algorithm SHA-1[14][15], and cryptographic key sizes none[16] that meet the following: [26][27][17][18].

Application note 30 (taken from application note 20 from [17])

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 [13].

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

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/ ENC

The TSF shall perform secure messaging (BAC) – encryption and decryption[19] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[20] and cryptographic key sizes 112 bit[21] that meet the following: FIPS 46-3[28] and [13]; normative appendix 5, A5.3 [22] .

Application note 31 (taken from application note 21 from [17])

[13] [assignment: list of cryptographic operations]
[14] [assignment: cryptographic algorithm]
[15] [selection: *SHA-1 or other approved algorithms*]
[16] [assignment: *cryptographic key sizes*]
[17] [assignment: *list of standards*]
[18] [selection: FIPS 180-2 or other approved standards]
[19] [assignment: *list of cryptographic operations*]
[20] [assignment: *cryptographic algorithm*]
[21] [assignment: *cryptographic key sizes*]
[22] [assignment: *list of standards*]

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

FCS_COP.1/AUTH
Cryptographic operation – Authentication

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 algorithms Triple-DES[24],[25] and cryptographic key sizes 112bits[26],[27] that meet the following:[28][28],[29]:

Application note 32 (taken from application note 22 from [17])

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

FCS_COP.1/MAC
Cryptographic operation – Retail MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/MAC

[23] [assignment: *list of cryptographic operations*]
[24] [assignment: *cryptographic algorithm*]
[25] [selection: *Triple-DES, AES*]
[26] [assignment: *cryptographic key sizes*]
[27] [selection: *112, 128, 168, 192, 256*]
[28] [assignment: *list of standards*]
[29] [selection: *FIPS 46-3 [28] , FIPS 197 [29]*

The TSF shall perform secure messaging – message authentication code[30] in accordance with a specified cryptographic algorithm Retail MAC[31] and cryptographic key sizes 112 bit[32] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[33] .

Application note 33 (taken from application note 23 from [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/EMRTD
Cryptographic operation – Signature generation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of in user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/AA_GEN. FCS_CKM.4 Cryptographic key destruction: Fulfilled by FCS_CKM.4

FCS_COP.1.1/EMRTD

The TSF shall perform digital signature generation[34] in accordance with a specified cryptographic algorithm RSA PKCS#1 v1.5 and RSA PKCS#1-PSS and ECDSA with SHA-1 SHA-224 SHA-256, SHA-384, SHA-512[35] and cryptographic key sizes RSA 2048-4096 bits, ECC 160, 192, 224, 256, 320, 384, 521[36], that meet the following [13].[37],[38]

Application note 34 (from ST author)

The TOE performs digital signature generation with RSA. This SFR has been included in this security target in addition to the SFRs defined by the [17] claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed [17].

Application note 35 (from ST author)

The underlying Platform supports RSA and ECDSA signature algorithms and cryptographic key length 1024 bits to 4096 bits (RSA) and 160 bits to 521 bits (ECDSA). These key lengths are supported with equivalent implementation-level security measures. However, to defend against attackers with high attack potential, the actual key length chosen

[30] [assignment: *list of cryptographic operations*]
[31] [assignment: *cryptographic algorithm*]
[32] [assignment: *cryptographic key sizes*]
[33] [assignment: *list of standards*]
[34] [assignment: *list of cryptographic operations*]
[35] [assignment: *cryptographic algorithm*]
[36] [assignment: *cryptographic key sizes*]
[37] According to [13], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.
[38] [assignment: *list of standards*]

for use during the operational phase must be appropriate and in line with current cryptographic recommendations. When selecting the key length, consideration must be given to the expected lifetime of the TOE to ensure that the chosen cryptographic strength remains sufficient throughout the entire operational lifespan.

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

FCS_RND.1
Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1

The TSF shall provide a mechanism to generate random numbers that meet DRG.3 (high) according to AIS20 [16][39].

Application note 36 (taken from application note 24 from [17])

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

Application note 37 (taken from application note 25 from [17])

The Table 9 Used authentication mechanism provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [13], normative appendix 5, and [9]
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 Mechanism	FIA_API.1/AA	Defined in [13].

Table 9 Used authentication mechanism

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

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

FIA_UID.1
Timing of identification

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",
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.

Application note 38 (taken from application note 26 from [17])

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 may create 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. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

Application note 39 (taken from application note 27 from [17])

In the "Operational Use" phase the MRTD must not allow anybody to read the Integrated Circuit Card Serial Number (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's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more than one RFID. If this identifier is randomly selected it will not violate the OT.Identification.

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

FIA_UAU.1
Timing of authentication

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

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"[41]

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

FIA_UAU.1.2

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

Application note 40 (taken from application note 28 from [17])

The Basic Inspection System and the Personalization Agent authenticate themselves.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on Triple-DES or AES.[42],[43].
3. **Active Authentication according to [13]**

Application note 41 (taken from application note 29 from [17])

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

Application note 42 (taken from application note 30 from [17])

[41] [assignment: *list of TSF-mediated actions*]
[42] [assignment: *identified authentication mechanism(*s)]
[43] [selection*: Triple-DES, AES or other approved algorithms*]

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [13]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore, the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

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

FIA_UAU.5
Multiple authentication mechanisms

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

FIA_UAU.5.1

The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES or AES,[44],[45]

to support user authentication.

FIA_UAU.5.2

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s):
   the Basic Access Control Mechanism with the Personalization Agent Key,
   the Symmetric Authentication Mechanism with the Personalization Agent Key,[46]

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.[47]

Application note 43 (taken from application note 31 from [17])

In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP)' [18]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

[44] [assignment: *list of multiple authentication mechanisms*]
[45] [selection: *Triple-DES, AES*]
[46] [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]
[47] [assignment*: rules describing how the multiple authentication mechanisms provide authentication*]

AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [19] FIA_UAU.5.2).

Application note 44 (taken from application note 32 from [17])

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

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

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

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

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism.[48]

Application note 45 (taken from application note 33 from [17])

The Basic Access Control Mechanism specified in [13] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Application note 46 (taken from application note 34 from [17])

Note that in case the TOE should also fulfil [18] 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.

FIA_API.1/AA
Authentication Proof of Identity – travel document

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA

The TSF shall provide the Active Authentication Mechanism according to [13][49] to prove the identity of the TOE.[50]

Application note 47 (from the ST author)

The SFR FIA_API.1/AA has been included in this security target in addition to the SFRs defined by the [17] claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed [17].

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

FIA_AFL.1
Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when an administrator configurable positive integer within [1-127][51] unsuccessful authentication attempts occur related to BAC authentication protocol[52].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been surpassed[53], the TSF shall delay each following authentication attempt until the next successful authentication[54].

Application note 48 (from ST author)

Application note 35 of [17]: Applied.

6.1.4. Class FDP User Data Protection

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

[49] [assignment: *authentication mechanism*]
[50] [assignment: *authorized user or role*]
[51] [selection: [assignment: *positive integer number],an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[52] [assignment: *list of authentication events*]
[53] [assignment: *met or surpassed*]
[54] [assignment: *list of actions*]

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 [55] 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[56] .

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

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control
	FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

The TSF shall enforce the Basic Access Control SFP[57] to objects based on the following:

1) Subjects:
   a) Personalization Agent,
   b) Basic Inspection System,
   c) Terminal,
2) Objects:
   a) data EF.DG1 to EF.DG16 of the logical MRTD,
   b) data in EF.COM,
   c) data in EF.SOD,
3) Security attributes
   a) authentication status of terminals.[58]

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,

[55] [assignment: *access control SFP*]
[56] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[57] [assignment: *access control SFP*]
[58] [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. 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[59].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[60].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the rule:

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[61].

Application note 49 (taken from application note 36 from [17])

The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [18] for details).

Application note 50 (taken from application note 37 from [17])

FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

FDP_UCT.1
Basic data exchange confidentiality - MRTD

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1

[59] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[60] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[61] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

The TSF shall enforce the Basic Access Control SFP[62] to be able to transmit and receive[63] user data in a manner protected from unauthorised disclosure.

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

FDP_UIT.1
Data exchange integrity - MRTD

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[64] to be able to transmit and receive[65] user data in a manner protected from modification, deletion, insertion and replay errors[66].

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[67] has occurred.

6.1.5. Class FMT Security Management

Application note 51 (taken from application note 38 from [17])

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

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

FMT_SMF.1
Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No Dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

[62] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[63] [selection*: transmit, receive*]
[64] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[65] [selection*: transmit, receive*]
[66] [selection: *modification, deletion, insertion, replay*]
[67] [selection: *modification*, *deletion, insertion, replay*]

1. Initialization,
2. Pre-personalization,
3. Personalization[68].

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

FMT_SMR.1
Security roles

Hierarchical to:	No other components
Dependencies:	FIA_UID.1 Timing of identification.

FMT_SMR.1.1

The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System[69]

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application note 52 (taken from application note 39 from [17])

The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

FMT_LIM.1
Limited capabilities

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.

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

[68] [assignment: *list of management functions to be provided by the TSF*]
[69] [assignment: *the authorised identified roles*]

3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[70]

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

FMT_LIM.2
Limited availability

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

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 and
4. substantial information about construction of TSF to be gathered which may enable other attacks[71].

Application note 53 (taken from application note 40 from [17])

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.

Application note 54 (taken from application note 41 from [17])

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

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

FMT_MTD.1/INI_ENA
Management of TSF data – Writing of Initialization Data and Pre-personalisation Data

Hierarchical to:	No other components.

[70] [assignment: *Limited capability and availability policy*]
[71] [assignment: *Limited capability and availability policy*]

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[72] the Initialization Data and Pre-personalisation Data[73] to the Manufacturer[74].

Application note 55 (taken from application note 42 from [17])

The pre-personalisation Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

FMT_MTD.1/INI_DIS
Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS

The TSF shall restrict the ability to disable read access for users to[75] the Initialization Data[76] to the Personalization Agent[77].

Application note 56 (taken from application note 43 from [17])

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 within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalisation 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 "personalisation" 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

Hierarchical to:	No other components.

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

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[78] the Document Basic Access Keys[79] to the Personalization Agent[80].

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ

The TSF shall restrict the ability to read [81] the

1. Document Basic Access Keys
2. Personalization Agent Keys[82]
3. **Active Authentication Private Key**[83]

to none[84].

Application note 57 (taken from application note 44 from [17])

The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

Application note 58 (from the ST author)

A refinement has been added to this SFR to also cover the private key for the Active Authentication mechanism.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

[78] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[79] [assignment: *list of TSF data*]
[80] [assignment: *the authorised identified roles*]
[81] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[82] [assignment: *list of TSF data*]
[83] [assignment: *list of TSF data*]
[84] [assignment: *the authorised identified roles*]

FMT_SMR.1	Security roles: fulfilled by FMT_SMR.1

FMT_MTD.1.1/AAPK

The TSF shall restrict the ability to create, load[85] the Active Authentication Private Key[86] to the Personalisation Agent.[87]

Application note 59 (from the ST author)

This SFR has been included in this security target in addition to the SFRs defined by the [17] claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed [17].

6.1.6. Class FPT Protection of the Security Functions

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

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

FPT_EMS.1
TOE Emanation

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

FPT_EMS.1.1

The TOE shall not emit information about IC Power consumption and command execution time[88] in excess of non-useful information[89] enabling access to Personalization Agent Key(s) [90] and Document Basic Access Keys[91] and Active Authentication Private Key[92].

FPT_EMS.1.2

[85] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[86] [assignment: *list of TSF data*]
[87] [assignment: *the authorised identified roles*]
[88] [assignment: *types of emissions*]
[89] [assignment: *specified limits*]
[90] [assignment: *list of types of TSF data*]
[91] [assignment: *list of types of user data*]
[92] [assignment: *type of users*]

The TSF shall ensure any unauthorized users[93] are unable to use the following interface smart card circuit contacts[94] to gain access to Personalization Agent Key(s) [95] and Document Basic Access Keys[96] and Active Authentication Private Key [97].

Application note 60 (Application note 45 taken from [17])

Applied.

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

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

FPT_FLS.1
Failure with preservation of secure state

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

FPT_FLS.1.1

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

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1[98]

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

FPT_TST.1
TSF testing

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

FPT_TST.1.1

The TSF shall run a suite of self tests during initial start-up, periodically during normal operation[99] to demonstrate the correct operation of the **TSF**[100].

[93] [assignment: *type of users*]
[94] [assignment: *type of connection*]
[95] [assignment: *list of types of TSF data*]
[96] [assignment: *list of types of user data*]
[97] [assignment: *type of users*]
[98] [assignment: *list of types of failures in the TSF*]
[99] [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]*]
[100] [selection: *[assignment: parts of TSF], the TSF*]

FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of TSF data[101].

FPT_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. [102]

Application note 61 (from ST author)

Application note 46 of [17]: Applied.

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

FPT_PHP.3
Resistance to physical attack

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

FPT_PHP.3.1

The TSF shall resist physical manipulation and physical probing[103] to the TSF[104] by responding automatically such that the SFRs are always enforced.

Application note 62 (taken from application note 47 from [17])

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

Application note 63 (taken from application note 48 from [17])

The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.2. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following component: ALC_DVS.2.

[101] [selection: *[assignment: parts of TSF], TSF data*]
[102] [selection*: [assignment: parts of TSF], TSF*]
[103] [assignment: *physical tampering scenarios*]
[104] [assignment: *list of TSF devices/elements*]

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

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

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

Table 10 Coverage of Security Objective for the TOE by SFR

The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by

the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the Personalization Agent Key or for reasons of interoperability with the [19] by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).

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

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

The security objective OT.Data_Int “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to 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, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The security objective OT.Data_Conf “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting, time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated

Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).

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

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

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

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

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

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

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

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

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

The security objective OT.Active_Auth_Proof “Proof of travel document’s chip authenticity” is ensured by the Active Authentication Mechanism [13] provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK. This key can either be written to the TOE as defined by FMT_MTD.1/AAPK or created on the TOE itself as supported by FCS_CKM.1/AA_GEN. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/EMRTD.

6.3.2. Dependency Rationale

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

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

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes,	Justification 2 for non-satisfied dependencies,
	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/ENC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1,
	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/AUTH	[FDP_ITC.1 Import of user data without security attributes,	Justification 3 for non-satisfied dependencies
	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/MAC	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_CKM.1,
	FDP_ITC.2 Import of user data with security attributes, or generation,	
	FCS_CKM.1 Cryptographic key	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/EMRTD	[FDP_ITC.1 Import of user data without	Fulfilled by FCS_CKM.1/AA_GEN

SFR	Dependencies	Support of the Dependencies
	security attributes, or FDP_ITC.2 Import of in user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control,	Fulfilled by FDP_ACC.1,
	FMT_MSA.3 Static attribute initialization	Justification 4 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or	Justification 5 for non-satisfied dependencies
	FTP_TRP.1 Trusted path],	
	[FDP_IFC.1 Subset information flow control or	
	FDP_ACC.1 Subset access control]	Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or	Justification 5 for non-satisfied dependencies
	FTP_TRP.1 Trusted path],	
	[FDP_IFC.1 Subset information flow control or	
	FDP_ACC.1 Subset access control]	Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1

SFR	Dependencies	Support of the Dependencies
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/AAPK	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FPT_EMS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

Table 11 Dependencies between the SFR for the TOE shows the dependencies between the SFR of the TOE.

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

Justification 1

The Active Authentication key pair cannot be deleted or regenerated.

Justification 2

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.

Justification 3

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

Justification 4

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

Justification 5

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.

6.3.3. Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, through 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 augmented to EAL4 has no dependencies to other security requirements

Dependencies ALC_DVS.2: no dependencies.

6.3.4. Security Requirements – Mutual Support and Internal Consistency

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

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

The dependency analysis in section 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 analysed, 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.

The additions made to include the Active Authentication Mechanism have been integrated in a consistent way to the model designed by the [17], e. g. by using the subject, object and operation definitions.

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

7. TOE summary specification

This chapter gives the overview description of the different TOE Security Functions composing the TSF. The mapping in-between the TSFs and SFRs can be found in Table 13 Mapping of SFRs to mechanisms of TOE.

7.1. TOE Security Functions

7.1.1. TSF.AccessControl

The TOE provides access control mechanisms that allow the maintenance of different security roles according to FMT_SMR.1 Security roles (Manufacturer, Personalisation Agent, Basic Inspection System) and the access control policies and functions (FDP_ACC.1, FDP_ACF.1).

Manufacturer role

The TOE restricts the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. Manufacturer is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

The TSF.AccessControl provides that the Manufacturer role is only valid in Pre-personalisation of OS according to [8].1.3.2 TOE Life Cycle.

Personalisation Agent role

Personalisation Agent is the only role with the ability:

- to disable read access for users to the Initialisation Data.
- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date.
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document after successful authentication (until the end of the Personalisation Phase).
- to read out the Initialisation Data and the Pre-personalisation Data.

The Personalisation Agent has the ability to create or load the Chip Authentication Private Key.

The TSF.AccessControl provides that the Personalisation Agent role is only valid in Personalisation phase of IDentity Applet life cycle.

Basic Inspection System role

The Basic Inspection System authenticate based on MRZ according to BAC protocol.

A Basic Inspection System is not authorized to access sensitive data such as biometric data (EF.DG3, EF.DG4)

The TSF.AccessControl provides that the Basic Inspection System role is only valid in Operational phase of IDentity Applet life cycle.

The TSF.AccessControl ensures that nobody is allowed to read all TOE intrinsic secret cryptographic keys stored in the travel document, such the Personalisation Agent Keys, and the Active Authentication Private Key

Any terminal is explicitly denied modifying any of the EF.DG1 to EF.DG16 of the logical travel document in operational phase

The TSF provides functionality for the following SFRs:

FDP_ACC.1: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FDP_ACF.1: It is a requirement about access control and authentication. The access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FIA_UAU.5: The requirement is about multiple authentication mechanisms. It is realized by TSF.Authenticate, TSF.AccessControl and the TSF.Platform.

FMT_MTD.1/AAPK This requirement about the restriction the ability of creation or loading the Active authentication key pair. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_READ This requirement about the restriction the ability of reading Document Basic Access Keys, Personalization Agent Keys and Active Authentication Private Key. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to write the Document Basic Access Keys to the Personalisation Agent. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

7.1.2. TSF.Authenticate

After activation or reset of the TOE no user is authenticated.

TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

The Platform contains a deterministic random number generator rated DRG.3 (high) according to AIS20 [16] that provides random numbers used for the authentication.

Proving the identity of the TOE is supported by the following means:

- Basic Access Control Authentication Protocol
- Passive Authentication Mechanism.

Proving the genuineness of the TOE is supported by the following means:

- Active Authentication Mechanism.

The TOE prevents reuse of authentication data related to:

- Basic Access Control Authentication mechanism
- Symmetric Authentication Mechanism based on AES or TDES;

The TOE implements the following authentication mechanism:

- Symmetric Authentication Mechanism;
- Basic Access Control;
- Active Authentication;

Symmetric Authentication Mechanism

In the Personalisation Phase of the TOE life cycle the TSF.Authenticate enforces to the Personalisation Agent authenticates itself to the TOE by usage of the Personalisation Agent Keys with the following Symmetric Authentication Mechanism.

The Symmetric Authentication mechanism has role in the Personalisation phase, when the TSF data for BAC are not available (MRZ).

The TOE knows two kinds of Symmetric Authentication Mechanism:

- The first one is based on Global Platform keys.
- The second one is based on Personalization Agent Key (ISO secure messaging).

BAC

Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD.

Basic Access Control protocol based on ISO/IEC 11770-2 key establishment mechanism 6.

The BAC uses MRZ, which are not effectively represent secrets, but are restricted revealable.

TSF.Authenticate provides after successful run of BAC the secure messaging (confidentiality, integrity and authenticity of communication) and for the terminal the Basic Inspection System role.

Active Authentication

TSF.Authenticate is able to Active Authentication Mechanism, which is an alternative to the Chip Authentication for proof the genuineness the TOE (this security feature prevents cloning the TOE).

Active Authentication is based on a challenge-response protocol which proves the knowledge of the Active Authentication Private Key of the TOE.

The Active Authentication Key Pair is a chip individual key pair, which contains:

- Active Authentication Public Key stored in EF.DG15 and signed by Document Signer (proofed the authenticity by passive authentication). The signature is in Documents Security Objects.
- Active Authentication Private Key stored in the secure memory (provided by the Platform) of the TOE.

Prerequisites of the Active Authentication are the following:

- Successful BAC and Passive Authentication.

Active Authentication is not mandatory, but optional.

The TSF provides functionality for the following SFRs:

FDP_ACC.1: It is a requirement about access control and authentication, the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FDP_ACF.1: It is a requirement about access control and authentication. The access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FIA_AFL.1: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF.Authenticate and TSF.SecureManagement.

FIA_UAU.4: The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF.Authenticate. For fresh random number is generated by the TSF.Platform.

FIA_UAU.5: The requirement is about multiple authentication mechanisms. It is realized by TSF.Authenticate, TSF.AccessControl and the TSF.Platform.

FIA_UAU.6 This requirement is about the reauthentication in the secure messaging and it is provided by the TSF.Authenticate, TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FMT_MTD.1/AAPK This requirement about the restriction the ability of creation or loading the Active authentication key pair. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_READ This requirement about the restriction the ability of reading Document Basic Access Keys, Personalization Agent Keys and Active Authentication Private Key. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to write the Document Basic Access Keys to the Personalisation Agent. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

FIA_API.1/AA: The requirement is about the Active Authentication, which is provided by TSF.Authenticate and TSF.CryptoKey and the TSF.Platform.

7.1.3. TSF.SecureManagement

The TSF.SecureManagement is responsible for the secure management of the security attributes, data and functions.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

The TSF provides functionality for the following SFRs:

FIA_AFL.1 This requirement about the authentication failure handling. It is provided by TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/AAPK This requirement about the restriction the ability of creation or loading the Active authentication key pair. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_READ This requirement about the restriction the ability of reading Document Basic Access Keys, Personalization Agent Keys and Active Authentication Private Key. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_MTD.1/KEY_WRITE: This requirement is about restriction of the ability to write the Document Basic Access Keys to the Personalisation Agent. It is provided by TSF.AccessControl TSF.Authenticate and TSF.SecureManagement.

FMT_SMF.1: The requirement is about performable management functions, which is provided by TSF.SecureManagement and partly used the TSF.Platform

7.1.4. TSF.CryptoKey

Key Generation

The TSF.CryptoKey provides the following key generation:

Active Authentication

ECC and RSA are supported key generation algorithm by TSF.CryptoKey.

RSA PKCS#1 v2.2, RSA PKCS#1-PSS and ECDSA are supported digital signature creation cryptographic algorithm.

The Active Authentication Private Key is stored in the chip secure memory (provided by TSF.Platform) and the Active Authentication Public Key is stored in EF.DG15 (protected by Passive Authentication).

BAC

Key Establishment Mechanism: ISO/IEC 11770-2 key establishment mechanism 6.

BAC Session keys derivation: 3DES session keys in CBC mode for message encryption and message authentication (BAC-K_{MAC}, BAC-K_{ENC}).

Key Usage

The Personalisation Agent Symmetric Authentication Mechanism:

- In case of secure messaging (ISO) scenario, by an off-card entity having the SK.PERS key contained, by IDentity instance. $SK._{PERS}$ is created in the Configuration Phase.
- In case of secure messaging (GP) scenario by an off-card entity having the IDentity instance's associated Security Domain keys, which have to be set unique value for each individual card during the Operating System (JCOP 4.5) pre-personalisation.

A successfully authenticated Personalisation Agent is allowed to change the Personalisation Agent Keys. The Personalization Agent Keys are stored by the Platform.

The Active Authentication Key Pair is unchangeable in the operation phase. The TSF.CryptoKey support the Active Authentication and it is responsible for the digital signature creation.

The TSF.CryptoKey is responsible for the cryptographic operation related to the secure messaging.

The TSF.CryptoKey prevents to reuse ephemeral key pairs and the session keys by freshly generated random number (provided by TSF.Platform (DRG.3)).

Key Destruction

The TSF.CryptoKey is responsible for destroying cryptographic keys in the following events:

i. $SK._{PERS}$ key is automatically destroyed and not available any more in Operational Phase.
ii. the BAC Session Keys:
    a. after detection of an error in verification of the MAC of a received command,
    b. any session keys before starting the communication with the terminal in a new power-on-session.

The TSF.CryptoKey uses the functionalities of the TSF.Platform in order to destroy the keys.

The TSF provides functionality for the following SFR:

FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and it uses the functionalities of TSF.Platform.

FCS_CKM.1/AA_GEN: The SFR requires generation of cryptographic keys (for Active Authentication). It is realized by TSF.CryptoKey, and it uses the functionalities of TSF.Platform.

FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FCS_COP.1/AUTH: Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/MAC: Requires use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_COP.1/ENC: Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/SHA: Requires use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/EMRTD Requires use of cryptographic operation (digital signature generation). It is provided by the TSF.CryptoKey and TSF.Platform.

FCS_RND.1: Requires use of operation which is provided by the TSF.Platform and TSF.CryptoKey.

FDP_UCT.1 This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FDP_UIT.1 This requirement is about the protection from modification, deletion, insertion and replay during the secure messaging. It is provided by the TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FIA_API.1/AA: The requirement is about the Active Authentication, which is provided by TSF.Authenticate and TSF.CryptoKey and the TSF.Platform.

FIA_UAU.6 This requirement is about the reauthentication in the secure messaging and it is provided by the TSF.Authenticate, TSF.CryptoKey and it uses the functionalities of TSF.Platform.

7.1.5. TSF.AppletParametersSign

During the IDentity Applet life cycle phases after LOADED state the IDentity Applet becomes the default Application and reaches SELECTABLE state. This is called the Initialization phase. During this phase the following steps are carried out:

- Applet configuration
- File creation (all control parameters)
- Object creation (all control parameters and some usage parameters)

Certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer and conform to the requirements. The Initialization state cannot be finished by reaching the INITIALIZED state, and the Personalization phase cannot be started without successful signature verification.

These signatures can be verified during the whole IDentity Applet life-cycle, thus the non-authorized changed become detectable by applying this SF.

The TSF provides functionality for the following SFRs:

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletParametersSign and TSF.Platform.

7.1.6. TSF.Platform

TSF.Platform provides the Manufacturer the capability to store the Initialisation and Pre-Personalisation Data in the audit records.

TSF.Platform provide functionalities (such as Crypto Library, random number generation, etc.) to the following:

- generate Active Authentication Key Pair;
- generate BAC session keys;
- perform BAC secure messaging – encryption/decryption and message authentication code;
- provide secure key destruction method functionality;
- perform digital signature generation (Active Authentication);
- provide mechanism to generate random numbers (DRG.3 (high));
- ensure that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to secret data;
- ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the objects of session keys and ephemeral private key;
- ensure that unauthorized are unable to use electrical contacts interface to gain access to secret data;
- preserve a secure state when exposure to operating conditions causing a TOE malfunction or failure is detected during self-tests;

- implements appropriate measures to continuously counter physical manipulation and physical probing;
- run a suite of self-tests to demonstrate the correct operation of the TSF and to verify the integrity of the TSF data and stored TSF executable code.

The TSF provides functionality for the following SFRs:

FAU_SAS.1: The SFR requires audit capabilities, which are provided by TSF.Platform.

FCS_CKM.1: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and TSF.Platform because it uses TSF.Platform functionalities.

FCS_CKM.1/AA_GEN Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_COP.1/EMRTD Requires use of cryptographic operation (digital signature generation). It is provided by the TSF.CryptoKey and TSF.Platform.

FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FCS_COP.1/ENC: Requires a use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_COP.1/AUTH: Requires use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_COP.1/MAC: Requires use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_COP.1/SHA: Requires use of cryptographic operation. It is provided by TSF.CryptoKey and TSF.Platform because it uses TSF.Platform functionalities.

FCS_RND.1: Requires use of operation which is provided by the TSF.Platform and TSF.CryptoKey.

FIA_API.1/AA: The requirement is about the Active Authentication, which is provided by TSF.Authenticate and TSF.CryptoKey and the TSF.Platform.

FIA_UAU.1 Requires use of the TSF.Platform functionalities.

FIA_UAU.4: The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF.Authenticate. For fresh random number is generated by the TSF.Platform.

FIA_UID.1 Requires use of the TSF.Platform functionalities.

FIA_UAU.5 The requirement is about multiple authentication mechanisms. It is realized by TSF.Authenticate, TSF.AccessControl and the TSF.Platform.

FIA_UAU.6 This requirement is about the re-authentication in the secure messaging and it is provided by the TSF.Authenticate, TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FDP_UCT.1 This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FDP_UIT.1 This requirement is about the protection from modification, deletion, insertion and replay during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FMT_LIM.1: The requirement is about restricting capabilities after TOE delivery, which is provided by TSF.Platform.

FMT_LIM.2: The requirement is about restricting availabilities after TOE delivery, which is provided by TSF.Platform.

FMT_SMF.1: The requirement is about performable management functions, which is provided by TSF.SecureManagement and partly the TSF.Platform.FMT_SMR.1: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

FMT_MTD.1/INI_ENA: This requirement is about restriction of the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. It is realized by TSF.Platform.

FMT_MTD.1/INI_DIS: This requirement is about restriction of the ability to read out the Initialisation Data to the Personalization Agent. It is realized by TSF.Platform.

FPT_EMS.1: Requires use of operation which is provided by the TSF.Platform.

FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF.Platform.

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletParametersSign and TSF.Platform.

FPT_PHP.3: Requires resistance to physical manipulation and probing to the Platform. This is realized by the TSF.Platform.

7.2. Assurance Measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the [5] and [6].
AM_ALC	The life-cycle support of the TOE during its development and maintenance is described in the

	life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 12 References of Assurance measures

7.3. Fulfilment of the SFRs

The following table shows the mapping of the SFRs to security functions of the TOE.

	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FAU_SAS.1	-	-	-	-	-	X
FCS_CKM.1	-	-	-	X	-	X
FCS_CKM.1/AA_GEN	-	-	-	X	-	X
FCS_CKM.4	-	-	-	X	-	X
FCS_COP.1/SHA	-	-	-	X	-	X
FCS_COP.1/ENC	-	-	-	X	-	X
FCS_COP.1/AUTH	-	-	-	X	-	X
FCS_COP.1/MAC	-	-	-	X	-	X
FCS_COP.1/EMRTD	-	-	-	X	-	X
FCS_RND.1	-	-	-	X	-	X
FIA_UID.1	-	X	-	X	-	X
FIA_AFL.1	-	X	X	-	-	
FIA_API.1/AA	-	-	-	-	-	X
FIA_UAU.1	-	-	-	-	-	X
FIA_UAU.4	-	X	-	-	-	X
FIA_UAU.5	X	X	-	-	-	X
FIA_UAU.6	-	X	-	X	-	X
FDP_ACC.1	X	X	-	-	-	
FDP_ACF.1	X	X	-	-	-	
FDP_UCT.1	-	-	-	X	-	X
FDP_UIT.1	-	-	-	X	-	X
FMT_SMF.1	-	-	X	-	-	X
FMT_SMR.1	X	X	-	-	-	X
FMT_LIM.1	-	-	-	-	-	X
FMT_LIM.2	-	-	-	-	-	X
FMT_MTD.1/AAPK	X	X	X	-	-	-

FMT_MTD.1/INI_ENA	-	-	-	-	-	X
FMT_MTD.1/INI_DIS	-	-	-	-	-	X
FMT_MTD.1/KEY_WRITE	X	X	X	-	-	-
FMT_MTD.1/KEY_READ	X	X	X	-	-	-
FPT_EMS.1	-	-	-	-	-	X
FPT_TST.1	-	-	-	-	-	X
FPT_FLS.1	-	-	-	-	-	X
FPT_PHP.3	-	-	-	-	X	X

Table 13 Mapping of SFRs to mechanisms of TOE

7.3.1. Correspondence of SFR and TOE mechanisms

Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8. Glossary and Acronyms

For Glossary and Acronyms please refer to the corresponding section of [17].

9. Bibliography

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

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

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

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

[5] IDentity Applet Suite v4.0 Administrator's Guide

[6] IDentity Applet Suite v4.0 User's Guide Version

[7] JCOP 4.5 P71 Security Target Lite, Rev. 2.9, 5 September 2025

[8] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018

[9] BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 eMRTDs with BAC/PACEv2 and EACv1 - Version 2.20 26., February 2015

[10] BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 Protocols for electronic Identification, Authentication and trust Services (eIDAS) - Version 2.21, 21. December 2016

[11] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 Common Specifications – Version 2.21, 21. December 2016

[12] BSI TR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 4 Applications and Document Profiles – Version 2.21, 21. December 2016

[13] International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015

[14] International Civil Aviation Organization (ICAO) Supplemental Access Control for Machine Readable Travel Documents, Version – 1.1, 15. April 2014

[15] Security IC Platform Protection Profile Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007

[16] Bundesamt fuer Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitaetsklassen und Evaluations methodologie fuer deterministische Zufallszahlengeneratoren, Version 2.1, 2.12.2011.

[17] Protection Profile — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP), Version 1.10, BSI-CC-PP-0055, 25.03.2009

[18] Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, BSI-CC-PP-0056-V2-2012, 05.12.2012

[19] Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, BSI-CC-PP-0068-V2-2011, 02.11.2011

[20] EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

[21] EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

[22] BSI: Common Criteria Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20th, 2015

[23]CEN/TS 15480-2 – Identification card systems - European Citizen Card - Part 2: Logical data structures and card services

[24]European Card for e-Services and National e-ID Applications - IAS ECC, Revision 1.0.1, 21.03.2008

[25]Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73

[26]Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.

[27]JCOP 4.5 P71, User manual for JCOP 4.5 P71, User Guidance and Administrator Manual, NXP Semiconductors, Rev. 2.2 – 2025-06-05.

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

[29]Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTIONSTANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[30]Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[31]Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[32]NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) Security Target Rev. 2.0, 4 August 2025

[33]EN 419211-5:2013 - Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application

[34]NIST Special Publication 800-67 –Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Published November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce