SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option

Security Target Lite

NSCIB-CC-0189569

Common Criteria / ISO 15408 / EAL 4+

Document Version 1.5 • 2021-06-11

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
1.3	2021-05-05	Thomas Zeggel	ST-Lite based on ST version 1.3.
1.4	2021-06-02	Thomas Zeggel	ST-Lite based on ST version 1.4.
1.5	2021-06-11	Thomas Zeggel	ST-Lite based on ST version 1.5, classification "confidential" erased.

1 Introduction

1.1 ST/TOE Identification

Title:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option – Security Target Lite
Document Version:	v1.5
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control (BSI-CC-PP0055) [PP0055]
Product identification:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0
TOE identification:	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option
Javacard OS platform:	SECORA™ ID X v1.1 (SLJ52GxAyyyzX), NSCIB-CC-0031318-CR2 [Cert_Secora]
Security controller:	IFX_CCI_000010 [ST_IC], BSI-DSZ-CC-1079-2020-v2
TOE documentation:	Administration and user guide [Guidance]

1.2 ST overview

This document contains the security target for MRTD chips based on the BAC application of the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0. SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 is a set of Javacard applications intended to be used exclusively on the SECORA ID-X Javacard OS platforms, which is certified according to CC EAL 5+ [Cert_Secora]. SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 as well as the SECORA ID-X operating system are provided on a smart card chip based on the Infineon IFX_CCI_000010 security controller, which is itself certified according to CC EAL 6+ [Cert_IC].

This ST claims strict conformance to the Protection Profile *Machine Readable Travel Document with "ICAO Application", Basic Access Control (*BSI-CC-PP0055) [PP0055].

The main objectives of this ST are:

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

The assurance level for the TOE is CC EAL4 augmented with ALC_DVS.2.

1.3 TOE overview

The TOE is a Java Card (SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0) configured to provide a contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the according configuration it can be programmed according to the Logical Data Structure (LDS) and provides the Basic Access Control according to the ICAO document [ICAODoc].

1.4 TOE description

1.4.1 Overview of SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0

SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 is a set of Java Card applets for e-ID document applications built upon an underlying core library. The following *Table 1* provides an overview of the individual applications included in SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0:

Product / Application	**Specification**	**Configuration**[1]
ICAO MRTD application with Basic Access Control (BAC) and Supplemental Access Control (SAC)	ICAO Doc 9303	ePasslet3.5/MRTD-BAC
ISO File System application	ISO 7816	ePasslet3.5/ISO-FS
ISO Driving License application with Basic Access Protection (BAP) or Supplemental Access Control (SAC)	ISO 18013	ePasslet3.5/IDL-Basic
ISO Driving License application with Extended Access Protection (EAP) or Extended Access Control (EACv1)	ISO 18013	ePasslet3.5/IDL-Extended
ICAO MRTD application with Extended Access Control (EACv1)	ICAO Doc 9303, TR03110v1.11	ePasslet3.5/MRTD-EAC
Secure Signature Creation Device application supporting PKI utilization	ISO 7816, PKCS#15	ePasslet3.5/SSCD
Secure Signature Creation Device application supporting PKI utilization – Device with key import	ISO 7816, PKCS#15	ePasslet3.5/SSCD-IMP
EU Electronic Vehicle Registration application	EU Council Directive 1999/37/EC	ePasslet3.5/eVR
EU Electronic Health Insurance application	CWA 15974	ePasslet3.5/eHIC
German eID Document application	ICAO Doc 9303, TR03110v2.11, TR03127 v1.15	ePasslet3.5/GeID
Customizable eID Document application	ICAO Doc 09303 and TR03110v2.11	ePasslet3.5/GenID
EU Electronic Residence Permit application	TR03127 v1.15	ePasslet3.5/eRP

[1] The names of the configurations reflect that the TOE is based on version 3.5 of ePasslet suite.

Table 1: Configurations of the SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0. Please note that not all configurations are certified according to Common Criteria. ***The TOE of this ST is marked in yellow****.*

These configurations are based on one or more predefined applets; different configurations might use the same underlying applet.

The whole applet code resides in the Flash memory; the applets providing these different configurations are instantiated into Flash memory. Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations. Such additional functionality is independent of the functionality of the TOE as described in this security target and the guidance manuals. This is ensured by the isolation properties of the Java Card platform.

A common combination could be an ICAO MRTD applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application.

The following configurations are certified according to Common Criteria:

- configuration providing Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC); this is the TOE of this security target;
- configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE; this TOE is defined in a separate security target;
- configuration providing Secure Signature Creation Device with key generation; this TOE is defined in a separate security target,
- configuration providing Secure Signature Creation Device with key import; this TOE is defined in a separate security target.

Combinations of certified and non-certified applications are possible.

Via configuration the instanciated applets can be tied to the contactless and/or the contact interface, respectively.

1.4.2 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the MRTD-BAC configuration it can be programmed according to the Logical Data Structure (LDS) and provides the Basic Access Control according to the ICAO document [ICAODoc]. The TOE consists of

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities,
- the platform with the Java Card operation system SECORA ID-X (SLJ52GxAyyyzX; please refer to the platform security target [ST_SECORA] for details of this designation),
- the guidance documentation of SECORA ID-X (SLJ52GxAyyyzX) according to [ST_SECORA], section 1.4.1.4.
- SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration[2] providing Machine Readable Travel Document with „ICAO Application", Basic Access Control,

[2] The term "configuration" is used for the different instantiated applets of the SECORA™ ID X Applet Collection with ePasslet Suite by cryptovision GmbH, version 1.0 and the files and keys with its access conditions, created before the operational use stage.

- the associated guidance documentation: Administrator and User Guidance [Guidance] in PDF format.

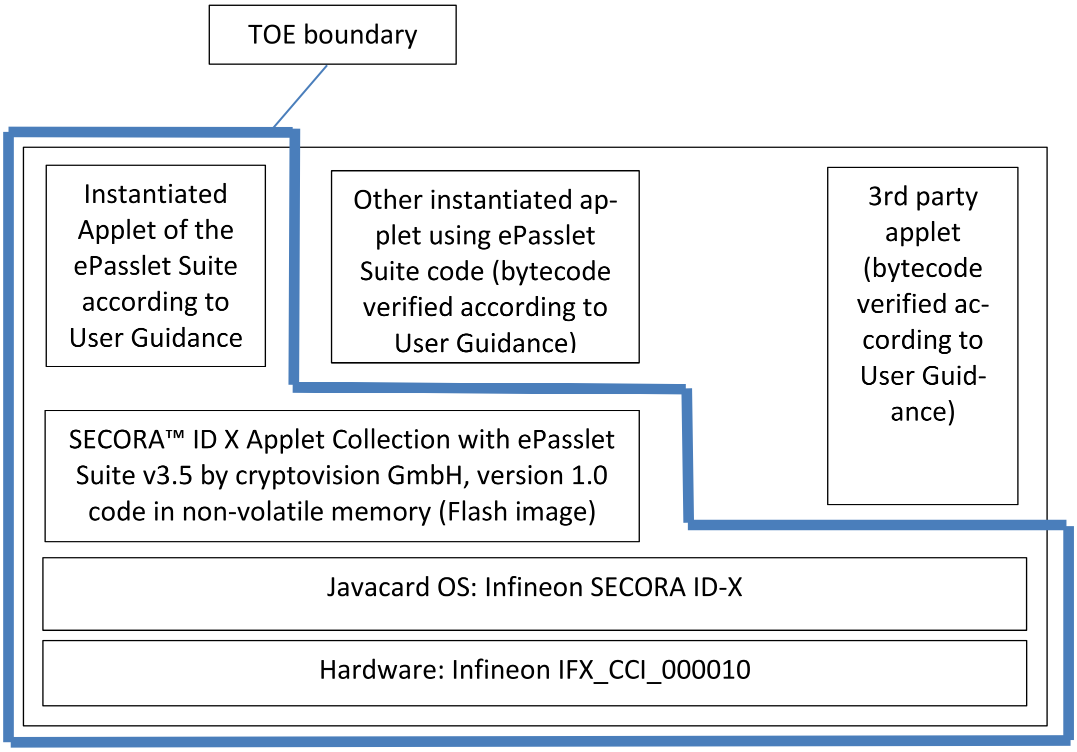


Figure 1: Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the certified hardware and Javacard OS. Besides the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 code in non-volatile memory and the applet instantiated from it which forms the TOE of this security target, it may also contain additional applets which are not part of the TOE.

The TOE's functionality claimed by this Security Target is realized by the SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 in the MRTD-BAC configuration only.

1.4.3 TOE package types and forms of delivery

The TOE can be delivered in the following forms:

- Packaged as
  - contact based modules
  - dual interface modules
  - contactless modules
- Packageless as sawn or unsawn wafer

The TOE supports Coil on Module antennas for dual interface modules [ST_SECORA].

The delivery is carried out in the following form:

TOE component	Delivered format	Delivery method	Comment

Underlying platform with SECORA™ ID X Applet Collection	Packaged as • contact based modules • dual interface modules • contactless modules Packageless as sawn or unsawn wafer	Postal transfer in cages	All materials are delivered to distribution centers in cages, locked.
All User Guidance documents including the SECORA ID-X guidance documentation	Personalized PDF	SecureX transfer	

1.4.4 TOE identification

Identification of the platform is performed by the procedure according to [AGD_PRE].

Once the platform is identified correctly, the correct version of the Java card layer of the TOE (SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0) can be verified as descibed in [Guidance].

1.4.5 TOE usage and security features for operational use

This paragraph is directly based on the corresponding paragraph in the protection profile [PP0055].

A state or organisation issues a MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity.

The MRTD 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 MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD.

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

Within this security target the MRTD is viewed as a unit of

- the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:
  (1) the biographical data on the biographical data page of the passport book,
  (2) the printed data in the Machine-Readable Zone (MRZ) and
  (3) the printed portrait.
- the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO-Doc] as specified by ICAO on the contactless integrated circuit. Via the contactless interface of the integrated circuit, the following data including (but not limited to) personal data of the MRTD holder are accessible:
  (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

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

(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[3]

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

(5) the document security object.

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

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

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

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

This security target addresses the protection of the logical MRTD (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 mechanism.

The Basic Access Control is a security feature that shall be mandatory implemented by the TOE. The inspection system (i) reads optically the MRTD, (ii) 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 [ICAODoc], normative appendix 5.

1.4.6 Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data.
- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS. The supported crypto mechanisms are:
    - Triple-DES for encryption/decryption and MAC calculation
    - SHA-1 for key derivation
- TSF_SecureMessaging realizes a secure communication channel with MACs and encryption based on Triple-DES (112 bit key length).

[3] These additional biometric reference data are optional

- TSF_Auth_Sym performs an authentication mechanism based on TDES used for BAC and based on AES for symmetric authentication with pre-shared keys for personalization.
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.
- TSF_OS contains all security functionalities provided by the certified platform (IC, crypto library, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform.

1.4.7 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases (subdivided into 7 steps). This paragraph is directly based on the corresponding paragraph in the protection profile [PP0055].

1.4.7.1 Phase 1: Development

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

(Step2) The software developer[4] 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 MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (NVM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

1.4.7.2 Phase 2: Manufacturing

(Step 3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The TOE delivery according to CC is the delivery of the IC (with the application code in NVM) from the IC manufacturer to the MRTD manufacturer.

(Step 4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book[5].

(Step 5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data.

Application Note 1: Creation of the application implies Applet instantiation.

In this step the final (but not yet personalized) MRTD is generated from the certified components according to the binding initialization and pre-personalization guidelines provided in [Guidance].

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

---

[4] Please note that in this ST the role software developer of the protection profile is subdivided into two separate roles: the operating system is developed by the OS software developer, and the MRTD application by the (MRTD) software developer.

[5] It is also possible that inlays with antenna are produced in this step.

1.4.7.3 Phase 3: Personalisation of the MRTD

(Step 6) The personalization of the MRTD includes (i) the survey of the MRTD holder biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD and their secure transfer to the Personalisation Agent, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) the writing the TSF Data into the logical MRTD and 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 (DG1), (ii) the digitised portrait (DG2), and (iii) the Document security object.

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

Application note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. application note 15) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Basic Authentication Control Key.

Application note 3: This Security Target and the underlying protection profile [PP0055] distinguish between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [PP0055], [ICAODoc]. This approach allows but does not enforce the separation of these roles. The TOE uses symmetric authentication keys for the personalization process. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment, e.g. by using hardware security module (HSM) for the storage of the authentication keys.

1.4.7.4 Phase 4: Operational use

(Step 7) The TOE is used as MRTD 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 used according to the security policy of the Issuing State but they can never be modified.

Application note 4: 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 5: The intention of the underlying PP [PP0055] is to consider at least the phases 1 and parts of phase 2 (i.e. Step 1 to Step 3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase 2 or later. 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 personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class.

Remark: This ST considers only phase 1 and parts of phase 2 (Steps 1 - 3) as part of CC evaluation under ALC.

1.4.8 Non-TOE hardware/software/firmware required by the TOE

This paragraph is directly based on the corresponding paragraph in the protection profile [PP0055].

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

2 Conformance claims

2.1 CC conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant
- Package conformant to EAL4 augmented with ALC_DVS.2.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004, [CC_4]

has to be taken into account.

The requirements for the evaluation of the TOE and its development and operating environment are those takenfrom the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2.

2.2 PP Claim

This security target claims strict conformance also to the Protection Profile *Machine Readable Travel Document with “ICAO Application”, Basic Access Control* (BSI-CC-PP0055) [PP0055]. No extensions have been made.

The evaluation of the TOE uses the result of the CC evaluation of the chip platform claiming conformance to the PP [PP_Javacard]. The hardware part of the composite evaluation is covered by the certification report [Cert_IC]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the Javacard OS. The Javacard OS part of the composite evaluation is covered by the certification reports [Cert_Secora].

2.3 Statement of Compatibility concerning Composite Security Target

2.3.1 Assessment of the Platform TSFs

The following table lists all Security Functionalities of the underlying Platform ST and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

Platform TSF-group	Correspondence in this ST	References/Remarks
SF.Firewall	No correspondence, internal Java card mechanism.	This security function provides an applet firewall. Each applet on the TOE must have been passed the Bytecode Verifier in order to ensure correct applet isolation.
SF.RIP	TSF_Secret	This security function ensures that sensitive information are made unavailable after usage by overwriting them with zeros or random values.
SF.Rollback	No correspondence, internal Java card mechanisms.	This security function implements atomicity and rollback mechanism for Global Platform management functions.
SF.SCP	TSF_SecureMessaging, TSF_Crypto (regarding Secure Messaging)	The TOE implements secure channel protocols according to [GP_v23], chapter 10. The protocols SCP02 and SCP03 are supported.
SF.CM	TSF_Access, TSF_Admin	This security function implements an access control policy for Global Platform card management functions according to [GP_v23], chapters 9.3 – 9.6.
SF.Physical	TSF_Integrity, TSF_Secret	This security function provides means to protect SFRs against physical tampering and leakage.
SF.CS	TSF_Crypto	This security function provides the cryptographic services for applets.

Table 2: Relevant platform TSF-groups and their correspondence

2.3.2 Assessment of the Platform SFRs

The following table provides an assessment of all Platform SFRs. The Platform SFRs are listed in the order used within the security target of the platform [ST_Secora].

Platform SFR	Correspondence in this ST	References/Remarks
CoreG_LC Security Functional Requirements (chapter 7.2.1 in platform ST)		
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FDP_IFC.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_IFF.1/JCVM	No correspondence	Out of scope (internal Java Virtual Machine). No contradiction to this ST.
FDP_RIP.1/OBJECTS	No correspondence.	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FMT_MSA.1/JCRE	No correspondence	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FMT_MSA.1/JCVM	No correspondence	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FMT_MSA.2/FIREWALL-JCVM	No correspondence	Out of scope (internal Java Card Fire-wall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradic-tion to this ST.
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (internal Java Card Fire-wall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradic-tion to this ST.
FMT_MSA.3/JCVM	No correspondence	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FMT_SMF.1	No correspondence	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FMT_SMR.1	No correspondence	Out of scope (internal Java Card Fire-wall). No contradiction to this ST.
FCS_CKM.1 (FCS_CKM.1.1/RSA, FCS_CKM.1.1/EC, FCS_CKM.1.1/AES, FCS_CKM.1.1/TDES)	No crrespondence.	Out of scope. The TOE uses the spe-cific Document Basic Access Key Der-ivation Algorithm. There are no con-tradictions to this ST.
FCS_CKM.2	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.
FCS_CKM.3	No correspondence	Out of scope (managed within Java Card OS). No contradiction to this ST.
FCS_CKM.4	FCS_CKM.4	The requirements are compatible (clearKey method, physically over-writing the keys). Thus, all internal Java Card key objects fulfill the re-quirement of this ST. There are no contradictions.

Platform SFR	Correspondence in this ST	References/Remarks
FCS_COP.1 (FCS_COP.1.1/JCAPI, FCS_COP.1.1/SCP, FCS_COP.1.1/SM)	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC	The requirements of this ST are equivalent to a subset of the platform requirements: FCS_COP.1/SHA of this ST corresponds to the platform SFR FCS_COP.1.1/JCAPI/HASH; FCS_COP.1/ENC corresponds to the platform SFR FCS_COP.1.1/JCAPI/TDES-ENC; FCS_COP.1/AUTH corresponds to the platform SFR FCS_COP.1.1/JCAPI/AES-ENC; FCS_COP.1/MAC corresponds to the platform SFR FCS_COP.1.1/JCAPI/TDES-MAC. No contradictions to this ST.
FDP_RIP.1/ABORT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/APDU	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/bArray	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/KEYS	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/TRANSIENT	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/FIREWALL	No correspondence.	Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST.
FAU_ARP.1	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. Internal counter for security violations complement Java Card OS mechanisms-No contradiction to this ST.
FDP_SDI.2	FPT_FLS.1, FPT_PHP.3	Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. No contradiction to this ST.
FPR_UNO.1	FPT_EMSEC.1	Not directly corresponding, but relevant for the fullfillment of FPT_EMSEC.1. No contradiction to this ST.
FPT_FLS.1	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of

Platform SFR	Correspondence in this ST	References/Remarks
		the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
FPT_TDC.1	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_ATD.1/AID	No correspondence.	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.2/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_USB.1/AID	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.1/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MTD.3/JCRE	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
INSTG Security Functional Requirements (chapter 7.2.2 in platform ST) This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime.		
FDP_ITC.2/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_RCV.3/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/Installer	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ADELG Security Functional Requirements (chapter 7.2.3 in platform ST) This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime.		
FDP_ACC.2/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_RIP.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FMT_SMR.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ADEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
ODELG Security Functional Requirements (chapter 7.2.4 in platform ST) The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.		
FDP_RIP.1/ODEL	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/ODEL	FPT_FLS.1	The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction to this ST.
CARG Security Functional Requirements (chapter 7.2.5 in platform ST) This group includes requirements for preventing the installation of packages that has not been bytecode verified, or that has been modified after bytecode verification. All SFRs of the platform are mapped to SFRs in CMGRG.		
CMGR Security Functional Requirements (chapter 7.2.6 in platform ST)		
FDP_UIT.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ROL.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FTP_ITC.2/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FPT_FLS.1/CCM	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FCS_COP.1/DAP	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACC.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_ACF.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMR.1/SD	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.

Platform SFR	Correspondence in this ST	References/Remarks
FTP_ITC.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FCO_NRO.2/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFC.2/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FDP_IFF.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_MSA.3/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FMT_SMF.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UID.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UAU.1/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
FIA_UAU.4/SC	No correspondence	Out of scope (internal Java Card functionality). No contradiction to this ST.
SCPG Security Functional Requirements (chapter 7.2.7 in platform ST) The group SCPG contains the security requirements from the underlying platform. The following SFRs are taken from [ST_IC]. Their exact definition will not be repeated here. For details, please see [ST_IC].		
FPT_PHP.3	FPT_PHP.3 FPT_EMSEC.1	The fulfillment of the SFR in this ST is based on the platform SFR (together with additional countermeasures).
FPT_TST.1	FPT_TST.1	The SFR of this ST is directly fulfilled by the platform SFR. No contradiction to this ST.
FCS_RNG.1	FCS_RND.1	In this ST, random numbers according to AIS20 class PTG.3 are required. The platform generates random numbers with a defined quality metric that can be used directly.

Table 3: Assessment of the platform SFRs.

2.3.3 Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

Platform Objective	Correspondence in this ST	References/Remarks
O.SID	No correspondence	Out of scope. No contradiction to this ST.

Platform Objective	Correspondence in this ST	References/Remarks
O.FIREWALL	No correspondence	Out of scope. No contradiction to this ST.
O.GLOBAL_ARRAYS_CONFID	OT.Data-Confidentiality	No contradiction to this ST.
O.GLOBAL_ARRAYS_INTEG	OT.Data-Integrity	No contradiction to this ST.
O.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
O.OPERATE	No correspondence	Out of scope. No contradiction to this ST.
O.REALLOCATION	No correspondence	Out of scope. No contradiction to this ST.
O.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
O.ALARM	No correspondence	Out of scope. No contradiction to this ST.
O.CIPHER	O.CIPHER	No correspondence
O.KEY-MNGT	O.KEY-MNGT	No correspondence
O.PIN-MNGT	No correspondence	Out of scope. No contradiction to this ST.
O.TRANSACTION	No correspondence	Out of scope. No contradiction to this ST.
O.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.DELETION	No correspondence	Out of scope. No contradiction to this ST.
O.LOAD	No correspondence	Out of scope. No contradiction to this ST.
O.INSTALL	No correspondence	Out of scope. No contradiction to this ST.
O.CARD-MANAGEMENT	No correspondence	Out of scope. No contradiction to this ST.
O.COMMUNICATION	No correspondence	Out of scope. No contradiction to this ST.
O.SCP.IC	OT.Prot_Phys-Tamper	The objectives are related. No contradiction to this ST.
O.SCP.RECOVERY	OT.Prot_Malfunction	The objectives are related. No contradiction to this ST.
O.SCP.SUPPORT	No correspondence	Out of scope. No contradiction to this ST.
O.SCP.RNG	No correspondence	Out of scope. No contradiction to this ST.

Table 4: Assessment of the platform objectives.

2.3.4 Assessment of Platform Threats

The following table provides an assessment of all relevant Platform threats.

Platform Threat	Correspondence in this ST	References/Remarks
T.CONFID-APPLI-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.CONFID-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.CONFID-JCS-DATA	T.Information_Leakage	No contradiction to this ST.
T.INTEG-APPLI-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-CODE.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-APPLI-DATA	T.Forgery	No contradiction to this ST.
T.INTEG-APPLI-DATA.LOAD	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-CODE	No correspondence	Out of scope. No contradiction to this ST.
T.INTEG-JCS-DATA	No correspondence	Out of scope. No contradiction to this ST.
T.SID.1	No correspondence	Out of scope. No contradiction to this ST.
T.SID.2	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.1	No correspondence	Out of scope. No contradiction to this ST.
T.EXE-CODE.2	No correspondence	Out of scope. No contradiction to this ST.
T.NATIVE	No correspondence	Out of scope. No contradiction to this ST.
T.RESOURCES	No correspondence	Out of scope. No contradiction to this ST.
T.DELETION	No correspondence	Out of scope. No contradiction to this ST.
T.INSTALL	No correspondence	Out of scope. No contradiction to this ST.
T.COMMUNICATION	No correspondence	Out of scope. No contradiction to this ST.
T.UNAUTHORIZED_CARD_MNGT	No correspondence	Out of scope. No contradiction to this ST.
T.LIFE_CYCLE	T.Phys-Tamper	No contradiction to this ST.
T.OBJ-DELETION	No correspondence	Out of scope. No contradiction to this ST.

Platform Threat	Correspondence in this ST	References/Remarks
T.PHYSICAL	No correspondence	Out of scope. No contradiction to this ST.
T.RNG	No correspondence	Out of scope. No contradiction to this ST.

Table 5: Threats of the platform ST.

2.3.5 Assessment of Platform Organisational Security Policies

The Organisational Security Policy "OSP.VERIFICATION" focuses on the integrity of loaded applets, which is fulfilled by the TOE of this ST since the applet is loaded secured by platform security measures into the flash memory. This policy does not contradict to the policies of this ST.

2.3.6 Assessment of Platform Operational Environment

2.3.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

Platform Assumption	Relevance for Composite ST
A.APPLET	A.APPLET states that applets loaded post-issuance do not contain native methods. This assumption leads to appropriate directives in the user guidance [Guidance].
A.VERIFICATION	This assumption targets the applet code verification. Regarding post-issuance loading of third party applets, this assumption leads to appropriate directives in the user guidance [Guidance].

Table 6: Assumptions of the Platform ST.

2.3.6.2 Assessment of Platform Objectives for the Operational Environment

There are the following Platform Objectives for the Operational Environment that have to be considered.

Platform Objective for the Environment	Relevance for Composite ST
OE.APPLET	The platform objective for the environment states that applets loaded post-issuance do not contain native methods. This objective for the environment leads to appropriate directives in the user guidance [Guidance].
OE.VERIFICATION	The platform objective for the environment targets the applet code verification. This is fulfilled by the TOE of this ST; regarding third-party-code, this objective for the environment leads to appropriate directives in the user guidance [Guidance]. There it is stated that all applets loaded to the TOE have to be verified.
OE.CODE-EVIDENCE	The platform objective for the environment focusses on application code loaded pre-issuance or

	post-issuance. It has to be ensured that the loaded application has not been changed since the code verification. This objective for the environment leads to appropriate directives in the user guidance [Guidance].

Table 7: Platform Security Objectives and SFRs for the Operational Environment

3 Security problem definition

3.1 Introduction

3.1.1 Assets

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

3.1.1.1 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 [ICAODoc]. 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.DG14) is used by the inspection system for the Chip Authentication within the EAC protocol (which is not in the scope of the TOE). 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' [ICAODoc] the TOE described in the according protection profile [PP0055] 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.

3.1.1.2 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 traveler to prove his possession of a genuine MRTD.

3.1.2 Subjects

This security target considers the following subjects:

3.1.2.1 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 users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

3.1.2.2 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 of 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 [ICAODoc].

3.1.2.3 Terminal

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

3.1.2.4 Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. 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 6: This security target does not distinguish between the BIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

3.1.2.5 MRTD Holder

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

3.1.2.6 Traveler

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

3.1.2.7 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 7: 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.

3.2 Assumptions

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

3.2.1 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).

3.2.2 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.

3.2.3 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.

3.2.4 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 traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAODoc]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application note 8: According to [ICAODoc] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This Security Target and the underlying PP [PP0055] does not address Primary Inspection Systems, therefore the BAC is mandatory within this ST.

3.2.5 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' [ICAODoc], 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 9: 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.

3.3 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 below.

3.3.1 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

3.3.2 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

3.3.3 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

3.3.4 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 passportbook, 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 of 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.

3.3.5 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

3.3.6 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

3.3.7 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 functionalties 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 functionality. 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

3.3.8 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 Functionalities of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent:	having enhanced basic attack potential, being in possession of a legitimate MRTD
Asset:	confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

3.4 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 [CC_1], section 3.2).

3.4.1 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.

3.4.2 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.

3.4.3 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)[6] 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 [ICAODoc].

Application note 10: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAODoc]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

[6] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this Security Target.

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.

4.1.1 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 [ICAODoc] 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.DG3 to EF.DG16 are added.

Application note 11: 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 (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

4.1.2 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.

4.1.3 OT.Data_Conf Confidentiality of sensitive biometric reference 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 12: 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 Functionality 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' [ICAODoc] 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 Extended Access Control not covered by this security target. Thus the read access must be prevented even in case of a successful BAC Authentication.

4.1.4 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 13: 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.

4.1.5 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.

4.1.6 OT.Prot_Inf_Leak Protection against Information Leakage

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

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

Application note 14: 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.

4.1.7 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 high attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

4.1.8 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 15: 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.

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.

4.2.1.1 OE.MRTD_Manufact Protection of the MRTD Manufacturing

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

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

4.2.1.2 OE.MRTD_ Delivery Protection of the MRTD delivery

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

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

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

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

4.2.1.3 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.

4.2.1.4 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 to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAODoc].

4.2.1.5 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' [ICAODoc] 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.

4.2.2.1 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 CA 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 [ICAODoc].

4.2.2.2 OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveler as 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 CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

4.2.2.3 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).

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_Absue-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				X									X			
T.Skimming			X										X			
T.Eavesdropping			X													
T.Forgery	X	X					X					X		X	X	
T.Abuse-Func					X						X					
T.Information_Leakage						X										
T.Phys-Tamper							X									
T.Malfunction								X								
P.Manufact				X												
P.Personalization	X			X							X					
P.Personal_Data		X	X													
A.MRTD_Manufact									X							
A.MRTD_Delivery										X						
A.Pers_Agent											X					
A.Insp_Sys														X		X
A.BAC-Keys													X			

Table 8: 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 Functionalities for the initialization and the personalization are disabled and the Security Functionalities 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 high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** “Protection against Information Leakage”, **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” and **OT.Prot_Malfunction** “Protection against Malfunctions”.

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

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

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.

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 Component Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [PP0002], other components are defined in protection profile [PP0055].

5.1 Definition of the Family FAU_SAS

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

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

5.1.1 FAU_SAS Audit data storage

Family behavior

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

Component leveling

FAU_SAS Audit data storage	1

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

Management:	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: a list of audit information] in the audit records.

5.2 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.

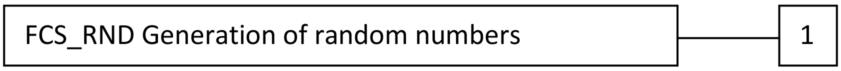
The family "Generation of random numbers (FCS_RND)" is specified as follows.

5.2.1 FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management:	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].

5.3 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.

5.3.1 FMT_LIM Limited capabilities and availability

Family behavior

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

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

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

FMT_LIM.1	**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 16: 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.

5.4 Definition of the Family FPT_EMSEC

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

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FCS_EMSEC TOE emanation	1

FPT_EMSEC.1 TOE emanation has two constituents:

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

6 IT 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 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying PP [PP0055] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to [PP0055].

Operations performed within this Security Target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

6.1 Security Definitions

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

Table 9: Security Definitions for the TOE

6.2 Security Functional Requirements for the TOE

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

6.2.1 Class Security Audit (FAU)

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

6.2.1.1 FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the ***Manufacturer*** with the capability to store the ***IC Identification Data*** in the audit records.

Application note 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 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).

6.2.2 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.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***Document Basic Access Key Derivation Algorithm*** and specified cryptographic key sizes ***112 bit*** that meet the following: ***[ICAODoc], normative appendix 5***.

Application note 18: 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 [ICAODoc], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAODoc], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

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

6.2.2.2 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 **physically overwriting the keys** [7] that meets the following: **none**[8].

Application note 19: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

6.2.2.3 FCS_COP.1 Cryptographic operation

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.

6.2.2.3.1 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

[7] [assignment: cryptographic key destruction method]

[8] [assignment: list of standards]

FCS_COP.1.1/SHA The TSF shall perform ***hashing*** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256** [9] and cryptographic key sizes ***none*** that meet the following: **FIPS 180-4**[10].

Application note 20: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [ICAO-Doc].

6.2.2.3.2 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*** in accordance with a specified cryptographic algorithm ***Triple-DES in CBC mode*** and cryptographic key sizes ***112 bit*** that meet the following: ***FIPS 46-3 [FIPS46-3] and [ICAODoc]; normative appendix 5, A5.3***.

Application note 21: 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.

6.2.2.3.3 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*** in accordance with a specified cryptographic algorithm **AES**[11] and cryptographic key sizes **128, 192 and 256 bit**[12] that meet the following: **FIPS 197** **[FIPS197]**[13].

Application note 22: 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). The TOE implements a symmetric authentication mechanism based on AES for the Personalization Agent as defined in [ISO18013-3], which is equivalent to the BAC protocol, but based on AES (in CBC mode for encryption and decryption following [NIST800-38A] and as a CMAC for message authentication following [NIST800-38B]).

6.2.2.3.4 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

---

9 [selection: SHA-1 or other approved algorithms]

10 [selection: FIPS 180-2 or other approved standards]

11 [selection: Triple-DES, DES, AES]

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

13 [selection: FIPS 46-3, FIPS 197]

	FDP_ITC.2 Import of user data with security attributes, or
	FCS_CKM.1 Cryptographic key generation]
	FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform secure messaging – ***message authentication code*** in accordance with a specified cryptographic algorithm ***Retail MAC*** and cryptographic key sizes ***112 bit*** that meet the following: ***ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)***.

Application note 23: 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.

6.2.2.4 FCS_RND.1 Random Number Generation

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

6.2.2.4.1 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 **the AIS 20/31 Class PTG.3 quality metric**[14].

Application note 24: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

Developer note: The corresponding platform SFR (FCS_RNG.1) states that the platform provides a hybrid deterministic random number generator (RNG) that fulfills the following:

- A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.
- If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
- The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 [AIS20] post-processing algorithm have been finished successfully or when a defect has been detected.
- The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
- The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
- The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post- processing algorithm shall not exceed its input data rate.

Thus the platform RNG implements AIS20/31 [AIS31] class PTG.3.

[14] [assignment: a defined quality metric]

6.2.3 Class Identification and Authentication (FIA)

Application note 25: The following *Table 10* provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-Doc], normative appendix 5, and [TR-03110]
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 Mecha-nism for Personalization Agent	FIA_UAU.4	AES with 128 up to 256 bit keys (cf. FCS_COP.1/AUTH)

Table 10: Overview of the authentication mechanisms used

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

6.2.3.1 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”*** 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 26: 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 27: In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’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. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

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

6.2.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 ***“Operational Use”*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note 28: 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).

6.2.3.3 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 **AES**[15][16].

Application note 29: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of the 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 30: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAODoc]. 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 stops further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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

6.2.3.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

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

[16] The TOE implements a symmetric authentication mechanism based on AES for the Personalization Agent as defined in [ISO18013-3], which is equivalent to the BAC protocol, but based on AES (in CBC mode for encryption and decryption following [NIST800-38A] and as a CMAC for message authentication following [NIST800-38B]).

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on **AES**[17] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) **the Symmetric Authentication Mechanism with the Personalization Agent Key**[18],
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the ***Document Basic Access Keys***.

Application note 31: In case the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control' [19] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The Personalization Agent could be authenticated by using the symmetric AES-based authentication mechanism or other (e.g. the Terminal Authentication Protocol using the Personalization Key, cf. [PP0056] FIA_UAU.5.2).[19]

Application note 32: 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).

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application note 33: The Basic Access Control Mechanism specified in [ICAODoc] 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 34: Note that in case the TOE should also fulfill [PP0056] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from

[17] [selection: Triple-DES, AES]

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

[19] Please note that not [PP0056] is in addition fulfilled by the TOE, but [PP0056v2].

the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

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

6.2.3.6 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 **10**[20] unsuccessful authentication attempts occur related to **BAC authentication**[21].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **met**[22], the TSF shall **delay each of the following authentication attempt until the next successful authentication attempt by an increasing amount of time** [23].

Application note 35 (examples) omitted.

6.2.4 Class User Data Protection (FDP)

6.2.4.1 FDP_ACC.1 Subset access control

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

6.2.4.1.1 FDP_ACC.1 Subset access control – Basic Access control

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*** 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***.

6.2.4.2 FDP_ACF.1 Security attribute based access control

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

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

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control

---

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

[21] [assignment: list of authentication events]

[22] [assignment: met or surpassed]

[23] [assignment: list of actions]

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the ***Basic Access Control SFP*** to objects based on the following:

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

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. ***the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD***.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the 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***.

Application note 36: The inspection system needs special authentication and authorization for read access to EF.DG3 and EF.DG4 not defined in this security target (cf. [PP0056] for details)[24].

6.2.4.3 FDP_UCT.1 Inter-TSF-Transfer

Application note 37: 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).

6.2.4.3.1 FDP_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

[24] Please note that not [PP0056] is in addition fulfilled by the TOE, but [PP0056v2].

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

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

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

6.2.4.4 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*** to be able ***to transmit and receive*** user data in a manner protected from ***modification, deletion, insertion and replay*** errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

6.2.5 Class FMT Security Management

Application note 38: 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).

6.2.5.1.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. ***Initialization,***
2. ***Pre-personalization,***
3. ***Personalization***.

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

6.2.5.1.2 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***.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note 39: 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)

6.2.5.1.3 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
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks

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

6.2.5.1.4 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.

Application note 40: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note 41: 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.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to ***write*** the ***Initialization Data and Pre-personalization Data*** to the ***Manufacturer***.

Application note 42: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to ***disable read access for users to the initialization Data*** to the ***Personalization Agent***.

Application note 43: 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-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

6.2.5.1.7 FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to ***write*** the ***Document Basic Access Keys*** to the ***Personalization Agent***.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to ***read*** the ***Document Basic Access Keys*** and ***Personalization Agent Keys*** to ***none***.

Application note 44: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.2.6 Class Protection of the Security Functions (FPT)

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

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

6.2.6.1.1 FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMSEC.1.1	The TOE shall not emit **variations in power consumption or timing during command execution**[25] in excess of **non-useful information**[26] enabling access to ***Personalization Agent Key(s)*** **and** **confidential user data**[27].
FPT_EMSEC.1.2	The TSF shall ensure ***any unauthorized users*** are unable to use the following interface: ***smart card circuit contacts*** to gain access to ***Personalization Agent Key(s)*** and **confidential user data**[28].

Application note 45: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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

6.2.6.1.2 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:

[25] [assignment: types of emissions]

[26] [assignment: specified limits]

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

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

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

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

6.2.6.1.3 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** [29] to demonstrate the ***correct operation of the TSF***.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data***.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application note 46: Further explanation of the protection profile [PP0055] applied, examples omitted.

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

6.2.6.1.4 FPT_PHP.3 Resistance to physical attack

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and ***physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.

Application note 47: 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 48: The SFRs “Non-bypassability of the TSF FPT_RVM.1” and “TSF domain separation FPT_SEP.1” are no longer part of [CC_2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.3 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following component:

ALC_DVS.2.

---

[29] [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]]

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Rationale

The following *Table 11* provides an overview for security functional requirements coverage.

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

Table 11: Coverage of the Security Objectives 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 SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the BAC mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [PP0055] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

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

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

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_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 blocking 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 (cf. Application note 30). In case of failed authentication attempts FIA_AFL.1 enforces blocking 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_EMSEC.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

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

6.4.2 Dependency Rationale

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

The following *Table 12* shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1,
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 1 for non-satisfied dependencies, Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 2 for non-satisfied dependencies justification 2 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 4 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 12: Dependencies between the SFR for the TOE

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

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

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

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

No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the 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.

6.4.3 Security Assurance Requirements Rationale

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

The selection of the component 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.

6.4.4 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 6.4.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.4.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.4.2 Dependency Rationale and 6.4.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.4.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE summary specification (ASE_TSS)

7.1 Security Functionality

7.1.1 TSF_Access: Access rights

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying SECORA ID-X Java Card platform (SF.CM).

Access is granted (or denied) in accordance to access rights that depend on appropriate identification and authentication mechanisms.

TSF_Access covers the following SFRs:

- FIA_UID.1 requires that the TSF shall allow reading specific data on behalf of the user to be performed before the user is identified, but shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.1 requires that the TSF shall allow reading of specific data on behalf of the user to be performed before the user is authenticated, but shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.4 requires that the TSF shall prevent reuse of authentication data. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a (1) Basic Access Control Authentication Mechanism and a (2) Symmetric Authentication Mechanism based on AES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Access realizes the appropriate control of the access rights.
- FIA_AFL.1 requires that the TSF shall detect when 10 unsuccessful authentication attempts related to BAC authentication has occurred, and that if this number has been met, the TSF shall delay each of the following authentication attempt until the next successful authentication attempt by an increasing amount of time. This is realized within TSF_Auth and TSF_Access.
- FDP_ACC.1: FDP_ACC.1.1 requires that the TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD. TSF_Access realizes the appropriate control of the access rights.
- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Basic Access Control SFP to objects based on the following: (1) Subjects: (a) Personalization Agent, (b) Basic Inspection System, (c) Terminal; (2) Objects: (a) data EF.DG1 to EF.DG16 of the logical MRTD, (b) data in EF.COM, (c) data in EF.SOD; (3) Security attributes: (a) authentication status of terminals. FDP_ACF.1.2 requires that 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, and (2) the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. FDP_ACF.1.3 requires that the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. This means that no other access possibilities exist. FDP_ACF.1.4 requires that 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. TSF_Access realizes the appropriate control of the access rights.

- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1) manufacturer, (2) personalization agent, and (3) basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.1: FMT_LIM.1.1 requires that the TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be disclosed or manipulated, (2) TSF data to be disclosed or manipulated, (3) software to be reconstructed and (4) substantial information about construction of TSF to be gathered which may enable other attacks. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.2: FMT_LIM.2.1 requires that 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. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1/KEY_WRITE: FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1/KEY_READ: FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none. TSF_Access realizes the appropriate control of the access rights.

7.1.2 TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in Phase 2 – while the actual applet is not yet present – is based on the card manager of the SECORA ID-X Java Card platform (SF.CM). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FAU_SAS.1: FAU_SAS.1 requires that the TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records. This is realized by TSF.Admin.
- FMT_SMF.1: FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1) initialization, (2) pre-personalization, and (3) personalization. This is realized within TSF_Admin.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1) manufacturer, (2) personalization agent, and (3) basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Admin provides the according storage area for manufacturing data, pre-personalization data and personalization data.

7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.CS of the underlying Java Card OS.

TSF_Secret covers the following SFRs:

- FCS_CKM.4: FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys by method (e.g. clearKey of [JCRE]) or automatically on applet deselection. This is mainly realized in the security functionalities provided by TSF_Secret (and TSF_OS).
- FMT_MTD.1/KEY_READ: FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none. This is realized within TSF_Secret.

7.1.4 TSF_Crypto: Cryptographic operations

This Security Functionality performs high level cryptographic operations. The implementation is based on the Security Functionalities provided by TSF_OS.

The supported crypto mechanisms are:

- Triple-DES for encryption/decryption and MAC calculation
- SHA-1 for key derivation

TSF_Crypto covers the following SFRs:

- FCS_CKM.4: FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys by method (e.g. clearKey of [JCRE]) or automatically on applet deselection. This is realized in the security functionalities provided by TSF_OS and TSF_Secret. The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security functionality is provided by TSF_Crypto.
- FCS_COP.1.1/AUTH: FCS_COP.1.1/AUTH requires that the TSF shall perform symmetric authentication (encryption and decryption) in accordance with a specified cryptographic algorithm (AES) and cryptographic key sizes of 128, 192 and 256 bit that meet FIPS 197. This is realized by TSF_Crypto based on TSF_OS.
- FCS_COP.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with a message authentication code in accordance with a specified cryptographic algorithm (Retail MAC) and a cryptographic key size of 112 bit that meets ISO 9797. The algorithm is realized within TSF_Crypto, while TSF_OS provides the basic Triple-DES implementation and TSF_SecureMessaging provides the secure messaging protocol.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a Basic Access Control Authentication Mechanism and a Symmetric Authentication Mechanism based on AES to support user authentication. The according cryptographic functions are realized within TSF_Crypto (based on functions provided by TSF_OS).

7.1.5 TSF_SecureMessaging: Secure Messaging

This Security Functionality realizes a secure communication channel after successful authentication for personalization and BAC during operational use.

It uses MACs and encryption based on Triple-DES (112 bit key length).

TSF_SecureMessaging covers the following SFRs:

- FCS_COP.1.1/ENC : FCS_COP.1.1/ENC requires that the TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm (2-key-Triple-DES in CBC mode) and cryptographic key sizes of 112 bit that meet FIPS 46-3. This is realized within TSF_OS.

- FCS_COP.1.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with a message authentication code in accordance with a specified cryptographic algorithm (Retail MAC) and a cryptographic key size of 112 bit that meets ISO 9797. TSF_OS provides the basic cryptographic mechanisms.
- FIA_UAU.6 requires that 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. TSF_Access realizes the appropriate control of the access rights.
- FDP_UCT.1: FDP_UCT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure. TSF_Access realizes the appropriate control of the access rights.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors. TSF_Access realizes the appropriate control of the access rights.
- FDP_UIT.1: FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred. This is realized within TSF_SecureMessaging.

7.1.6 TSF_Auth: Authentication protocols

This Security Functionality realizes different authentication mechanisms.

7.1.6.1 TSF_Auth_Sym

TSF_Auth_Sym performs an authentication mechanism based on TDES used for BAC and based on AES used for symmetric authentication with pre-shared keys for personalization.

TSF_Auth_Sym covers the following SFRs:

- FIA_UID.1: FIA_UID.1.1 requires that the TSF shall allow to read the Initialization Data in Phase 2 “Manufacturing”, to read the random identifier in Phase 3 “Personalization of the MRTD”, and to read the random identifier in Phase 4 “Operational Use” on behalf of the user to be performed before the user is identified. The authentication mechanism leads to the identification and is provided by TSF_Auth.
- FIA_UAU.1: FIA_UAU.1.1 requires that the TSF shall allow to read the Initialization Data in Phase 2 “Manufacturing”, to read the random identifier in Phase 3 “Personalization of the MRTD”, and to read the random identifier in Phase 4 “Operational Use” on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The authentication mechanism is provided by TSF_Auth.
- FIA_UAU.4: FIA_UAU.4.1 requires that the TSF shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism, and Authentication Mechanism based on AES. The authentication mechanisms are provided by TSF_Auth.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a Basic Access Control Authentication Mechanism and a Symmetric Authentication Mechanism based on AES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user’s claimed identity according to specified rules. The authentication mechanisms are provided by TSF_Auth.
- FIA_AFL.1: FIA_AFL.1.1 requires that the TSF shall detect when 10 unsuccessful authentication attempts occur related to BAC authentication. FIA_AFL.1.2 requires that when the defined number of

unsuccessful authentication attempts has been met, the TSF shall delay each of the following authentication attempt until the next successful authentication attempt by an increasing amount of time. The authentication mechanism is provided by TSF_Auth.

- FDP_ACC.1: FDP_ACC.1.1 requires that the TSF shall enforce the Basic Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD. The authentication mechanism is provided by TSF_Auth.
- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Basic Access Control SFP to objects based on defined subjects, objects, security attributes. FDP_ACF.1.2 requires that the TSF shall enforce the defined rules to determine if an operation among controlled subjects and controlled objects is allowed. FDP_ACF.1.3 requires that no other access possibilities exist. FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on defined rules. The authentication mechanism for the Basic Access Control SFP is provided by TSF_Auth.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles manufacturer, personalization agent, and basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. The according authentication mechanism is provided by TSF_Auth.
- FMT_LIM.1: FMT_LIM.1.1 requires that 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 User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The according authentication mechanism is provided by TSF_Auth.
- FMT_LIM.2: FMT_LIM.2.1 requires that 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 User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The according authentication mechanism is provided by TSF_Auth.

7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists.

TSF_Integrity covers the following SFRs:

- FPT_FLS.1: FPT_FLS.1.1 requires that 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, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_Integrity.

7.1.8 TSF_OS: Javacard OS Security Functionalities

The Javacard operation system (part of the TOE) features the following Security Functionalities. The exact description can be found in the Java Card OS security target [ST_Secora]; the realization is partly based on the security functionalities of the certified IC platform:

- Applet firewall (SF.Firewalll)
- Secure overwriting of data (SF.RIP)
- Atomicity and rollback mechanism for Global Platform management functions (SF.Rollback)
- Secure channel protocols (SF.SCP)
- Access control policy for Global Platform card management functions (SF.CM)

- Security measures against physical tampering and leakage (SF.Physical)
- Cryptographic services for applets (SF.CS)
- Secure PIN compare functions and integrity protection of the PIN (SF.PIN)

Since the applet layer of the TOE is based on the Javacard OS, the realization of all TOE security functionalities and thus the fulfillment of all SFRs has dependencies to TSF_OS. The following items list all SFRs where TSF_OS has an impact above this level:

- FCS_CKM.1: FCS_CKM.1.1 requires that the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (Document Basic Access Key Derivation Algorithm) and specified cryptographic key sizes of 112 bit. This is realized within TSF_OS.
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized in the security functionalities provided by TSF_OS (and TSF_Secret). The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security functionality is provided by TSF_Crypto.
- FCS_COP.1.1/SHA: FCS_COP.1.1/SHA requires that the TSF shall perform hashing in accordance with a specified cryptographic algorithm (SHA-1 or SHA-256) that meets: FIPS 180-4. This is realized within TSF_OS.
- FCS_COP.1.1/ENC : FCS_COP.1.1/ENC requires that the TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm (2-key-Triple-DES in CBC mode) and cryptographic key sizes of 112 bit that meet FIPS 46-3. This is realized within TSF_OS.
- FCS_COP.1.1/AUTH: FCS_COP.1.1/AUTH requires that the TSF shall perform symmetric authentication (encryption and decryption) in accordance with a specified cryptographic algorithm (AES) and cryptographic key sizes of 128, 192 and 256 bit that meet FIPS 197. This is realized within TSF_OS.
- FCS_COP.1.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with a message authentication code in accordance with a specified cryptographic algorithm (Retail MAC) and a cryptographic key size of 112 bit that meets ISO 9797. TSF_OS provides the basic cryptographic mechanisms.
- FCS_RND.1.1: FCS_RND.1.1 requires that the TSF shall provide a mechanism to generate random numbers that meet the AIS 20 Class DRG.4 quality metric. This is realized within TSF_OS.
- FMT_LIM.1: FMT_LIM.1.1 requires that 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 User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The implementation is based on TSF_OS.
- FMT_LIM.2: FMT_LIM.2.1 requires that 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 User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The implementation is based on TSF_OS.
- FMT_MTD.1.1/INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer. The basic mechanisms are provided by TSF_OS.
- FMT_MTD.1.1/INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent. The basic mechanisms for this are provided by TSF_OS.

- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. The basic mechanisms are provided by TSF_OS.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none. The basic mechanisms are provided by TSF_OS.
- FPT_EMSEC.1.1 requires that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to Personalization Agent Key(s) and confidential user data. FPT_EMSEC.1.2 requires that the TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and confidential user data. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.
- FPT_FLS.1.1 requires that 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, and (2) failure detected by TSF according to FPT_TST.1. This is realized within TSF_OS (together with and TSF_Integrity).
- FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

7.2 Mapping of TOE Security Requirements and TOE Security Functionalities

Each TOE security functional requirement is implemented by at least one security functionality. The mapping of TOE Security Requirements and TOE Security Functionalities is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 7.1.

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FAU_SAS.1		X						
FCS_CKM.1								X
FCS_CKM.4			X	X				X
FCS_COP.1/SHA								X
FCS_COP.1/ENC					X			X
FCS_COP.1/AUTH				X				X
FCS_COP.1/MAC				X	X			X

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth	TSF_Integrity	TSF_OS
FCS_RND.1								X
FIA_UID.1	X					X		
FIA_UAU.1	X					X		
FIA_UAU.4	X					X		
FIA_UAU.5	X			X		X		
FIA_UAU.6					X			
FIA_AFL.1	X					X		
FDP_ACC.1	X					X		
FDP_ACF.1	X					X		
FDP_UCT.1					X			
FDP_UIT.1					X			
FMT_SMF.1		X						
FMT_SMR.1	X	X				X		
FMT_LIM.1	X					X		X
FMT_LIM.2	X					X		X
FMT_MTD.1	X	X						X
FMT_MTD.1/INI_ENA								X
FMT_MTD.1/INI_DIS								X
FMT_MTD.1/KEY_WRITE	X							X
FMT_MTD.1/KEY_READ	X		X					X
FPT_EMSEC.1								X
FPT_FLS.1							X	X
FPT_TST.1								X
FPT_PHP.3								X

Table 13: Mapping of TOE Security Requirements and TOE Security Functionalities.

8 References

In the following tables, the references used in this document are summarized.

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017; CCMB-2017-04-001.
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-002.
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017; CCMB-2017-04-003.
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017; CCMB-2017-04-004.

Protection Profiles

[PP0056v2]	Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 5.12.2012, BSI-CC-PP-0056-V2-2012, Bundesamt für Sicherheit in der Informationstechnik.
[PP0068v2]	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22.7.2014, BSI-CC-PP-0068-V2-2011-MA-01, Bundesamt für Sicherheit in der Informationstechnik.
[PP0084]	Security IC Platform Protection Profile, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.
[PP0055]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009.
[PP_Javacard]	Java Card Protection Profile - Open Configuration, Version 3.0 (May 2012), Published by Oracle, Inc.

TOE and Platform References

[ST_Secora]	Security target Infineon SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Rev1.3, 22 March 2021.
[Cert_Secora]	Certification Report SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Report number NSCIB-CC-0031318-CR2, 6 April 2021.
[ST_IC]	Security Target Lite BSI-DSZ-CC-1079-V2-2020 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG
[Cert_IC]	BSI-DSZ-CC-1079-V2-2020 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG, 16 June 2020.

[Guidance]	[Guidance] consists of three documents: (1) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card Applet Suite providing Electronic ID Documents applications. Guidance Manual. Document Version 1.0.9, 2021-06-02. (2) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) - Preparation Guidance (AGD_PRE). Document Version 1.0.5, 2021-05-05. (3) Secora ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) - Operational Guidance (AGD_OPE). Document Version 1.0.4, 2021-05-05.
[GP_CIC]	GlobalPlatform Card Common Implementation Configuration Version 1.0, February 2014
[GP_v23]	Global Platform Card Specification v2.3
[AGD_PRE]	SECORA ID X Administration Guide, Revision 1.50, 2021-02-05.

ICAO specifications

[ICAODoc]	ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization
[ICAO_SAC]	International Civil Avation Organisation, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 11, 2010

Cryptography

[TR-03110]	Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 20.03.2012[30]
[TR-ECC]	Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.
[ISO7816-4]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004
[AIS20]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[AIS31]	Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 31, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[ISO14888-3]	ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures withappendix – Part 3: Certificate-based mechanisms, 1999
[FIPS46-3]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25,

[30] This document version superseded by a newer one, but the one that is cited in the Protection Profile PP0056v2.

	U.S.DEPARTMENT OF COMMERCE/National Institute of Standards and Technlogy
[NIST800-20]	NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999
[FIPS180-2]	Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD(+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/NationalInstitute of Standards and Technology, 2002 August 1
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, March 2012
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTIONSTANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standardsand Technology, November 26, 2001
[ANSIX9.19]	ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996
[ANSIX9.62]	AMERICAN NATIONAL STANDARD X9.62-1999: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),September 20, 1998
[ISO9796-2]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[ISO15946]	ISO/IEC 15946. Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002.
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[ISO18013-3]	ISO/IEC 18013-3:2009 Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation (2009)
[NIST800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, National Institute of Standards and Technology, December 2001
[NIST800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005
[RFC4493]	Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006
[ISO11770-3]	ISO/IEC 11770 Part 3: Information technology- Security techniques - Key management: Mechanisms using asymmetric techniques
[Brainpool]	RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010; available at:http://tools.ietf.org/html/rfc5639
[FIPS186-3]	Digital Signature Standard (DSS) - FIPS PUB 186-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June 2009.[31]

[31] This document version superseded by a newer one, but the one that is cited in the Protection Profile PP0056v2.

[PKCS1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note Version 2.1
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography; BSI, Version 2.0, 28.6.2012

Glossary

Active authentication	Security mechanism defined in [ICAODoc] by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
AES	The AES (Advanced Encryption Standard) has been defined as a standard for symmetric data encryption. It is a block cipher with a block length of 128 bit and key lengths of 128, 192 and 256 bit.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Asymmetric cipher	Encryption procedures employing two different keys (in contrast to a symmetric cipher): one publicly known (public key) for data encryption and one key only known to the message receiver (private key) for decryption.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authentication	Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.
BAC	Basic access control. Security mechanism defined in [ICAODoc] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging.
Basic access keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAODoc]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Block cipher	An algorithm processing the plaintext in bit groups (blocks). Its alternative is called stream cipher.
CA	Certification authority
Certificate	see digital certificate
Certificate revocation list	A list of revoked certificates issued by a certificate authority
Certification authority	An entity responsible for registering and issuing, revoking and generally managing digital certificates
Country signing CA certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority. The C_{CSCA} is stored in the inspection system.
Country verifying CA	The country specific root of the PKI of Inspection Systems. It creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing country or organization in respect to the protection of sensitive biometric data stored in the MRTD.
CRL	see Certificate Revocation List
Cryptography	In the classical sense, the science of encrypting messages. Today, this notion comprises a larger field and also includes problems like authentication or digital signatures.

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

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

DES (Data Encryption Standard) symmetric 64 bit block cipher, which was developed (first under the name Lucifer) by IBM. The key length is 64 bit of which 8 bit serve for a parity check. DES is the classic among the encryption algorithms, which nevertheless is no longer secure due to its insufficient key length. Alternatives are Triple-DES or the successor AES.

Digital certificate A data set that identifies the certification authority issuing it, identifies its owner, contains the ower's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.

Digital signature The counterpart of a handwritten signature for documents in digital format. A digital signature grants authentication, integrity, and non-repudiation. These features are achieved by using asymmetric procedures.

Document verifier Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations

EAC Extended access control. Security mechanism identified in [ICAODoc]by which means the MTRD’s chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.

ECC (Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.

Elliptic curves A mathematical construction, in which a part of the usual operations applies, and which has been employed successfully in cryptography since 1985.

Fingerprint (digital) Checksum that can be used to easily determine the correctness of a key without having to compare the entire key. This is often done by comparing the hash values after application of a hash function.

Hash function A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value. Common hash functions are RIPEMD-160 and SHA-1, each having hash values with a length of 160 bit as well as the MD5, which is still often used today having a hash value length of 128 bit.

Inspection system A technical system 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.

Integrity	The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash-functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.
Javacard	A smart card with a Javacard operation system.
Key exchange	The use of symmetric cipher procedures requires that two communication partners decide on one joint key only known to themselves. The difficulty is that for the exchange of such information usually only partially secure channels exist. Additionally, protocols for key exchange must be prepared in such a way that only those pieces of information are exchanged which do not lead to knowledge of the real secret (the key). The most popular protocol of that type is diffie-Hellman, whose presentation in 1976 can be regarded as the birth of public key cryptography.
LDS	Logical data structure. The collection of groupings of data elements stored in the optional capacity expansion technology, defined in [ICAODoc].
MAC	Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy, requires its protection in a suitable way.
MRTD	Machnine-readable travel document. Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read.
MRZ	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods.
Non-repudiation	One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Passphrase	A long, but memorable character sequence (e.g. short sentences with punctuation) which should replace passwords as they offer more security.
Password	A secret character sequence whose knowledge is to serve as a replacement for the authentication of a participant. A password is usually short to really ensure that an attacker cannot guess the password by trial and error.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Personalization agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

PKI	Cf. Public Key Infrastructure
PP	Protection Profile
Private key	Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.
Pseudo random number	Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo-random number generators are used, which then should be initialized with a real random element (the so called *seed*).
Public key	Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.
Public key infrastructure (PKI)	Combination of hardware and software components, policies, and different procedures used to manage digital certificates.
Random numbers	Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead.
Secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
SFR	Security functional requirement.
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Smart card	A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.
SOD	Document Security Object (stored in EF.SOD). A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS).
ST	Security Target
Stream cipher	Symmetric encryption algorithm which processes the plaintext bit-by-bit or byte-by-byte. The other usually employed class of procedures comprises so called block cipher.
Symmetric cipher	Encryption procedure using the same key for enciphering and deciphering (or, in which these two keys can simply be derived from each other). One distinguishes between block ciphers processing plaintext in blocks of fixed length (mostly 64 or 128 bit) and stream ciphers working on the basis of single characters.

TOE	Target of evaluation.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
TSF	TOE security functionality.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.
X.509	Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system.