STARCOS 3.5 ID EAC+AA C1

Security Target Lite

Version 2.9

R&D

Author	Giesecke & Devrient GmbH
Status	Final
Rating	Public
Edition	26.07.2012

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
D-81607 München

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
D-81607 München

Contents

1 ST Introduction

1.1 ST Reference

Title: Security Target Lite STARCOS 3.5 ID EAC+AA C1

Reference: GDM_STA35_EAC_C1_ASE

Version 2.9 Status 26.07.2012

Origin: Giesecke & Devrient GmbH

CC Version: 3.1 (Revision 3)

Assurance Level: EAL4-augmented with the following assurance components: ALC_DVS.2 and AVA_VAN.5.

TOE: STARCOS 3.5 ID EAC+AA C1

TOE documentation:

- Guidance Documentation STARCOS 3.5 ID – Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.5 ID EAC+AA C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID EAC+AA C1
- Guidance Documentation for the Usage Phase STARCOS 3.5 ID EAC+AA C1

HW-Part of TOE: Infineon M7820 (Certificate: BSI-DSZ-CC-0813-2012) [33]. This TOE was evaluated against Common Criteria Version 3.1.

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control and Extended Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [5].

In the following chapters STARCOS 3.5 ID EAC+AA C1 stands for the Target of Evaluation (TOE). The related product is the STARCOS 3.5 ID EAC+AA C1 Card.

STARCOS 3.5 ID EAC+AA C1 consists of the related software in combination with the underlying hardware ('Composite Evaluation') including the STARCOS35PETABLES [36] and the GMA Verifier[1] [37] including its configuration file.

The TOE software is the STARCOS 3.5 ID operating system and the ePass application. The TOE hardware is the secure Infineon M7820 certified according to CC EAL5+ with the following configurations according to [33]:

[1] The GMA Verifier is not part of the TOE delivery. It is solely used by the MRTD Manufacturer for the correct installation of the TOE and therefore of no use for the Personalisation Agent.

- NVM: 36 kByte up to 128 kByte
- ROM: 280 kByte
- XRAM: 8 kByte
- SCP: Accessible
- Crypto2304T: Accessible
- Interfaces: ISO/IEC 14443

The sales names of the TOE hardware platform [33] and the corresponding TOE names of STARCOS 3.5 ID EAC+AA C1 are listed below:

sales name of M7820 [33]	TOE name of STARCOS 3.5 ID EAC+AA C1
SLE78CLX360P	STARCOS 3.5 ID EAC+AA C1/360
SLE78CLX800P	STARCOS 3.5 ID EAC+AA C1/800
SLE78CLX1280P	STARCOS 3.5 ID EAC+AA C1/1280

In addition to the BSI-PP-0056 [28] the STARCOS 3.5 ID EAC+AA C1 supports the Active Authentication mechanism [5].

The assurance level for the TOE is CC EAL4 augmented.

1.2.1 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the conformance claims for the Security Target.

Section 3 provides a discussion of the security problems for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the operational environment and the security objective rational to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 5 contains the extended component definitions.

Section 6 contains the security functional requirements and assurance requirements derived from the Common Criteria [1], Part 2 [2] and Part 3 [3], which must be satisfied and the security functional requirements rational. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 7 contains the TOE Summary Specification.

Section 8 provides information on used acronyms and glossary and the used references.

1.2.2 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [5] and providing the Basic Access Control and Extended Access Control according to the 'ICAO Doc 9303' [5] and BSI TR-03110 [29], respectively.

The TOE comprises of at least

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and
- the associated guidance documentation.

1.2.3 TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in 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 traveler 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.

For this security target the MRTD is viewed as unit of

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

(1) the biographical data on the biographical data page of the passport book,

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

(3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

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

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

(3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[2]

(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.

[2] These biometric reference data are optional according to [1]. The PP [28] assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

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) [5]. 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 sensitive biometrics as optional security measure in the ICAO Doc 9303 [5]. 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 Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [29] as an alternative to the Active Authentication stated in [5].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this ST as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfil the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' [27]. Due to the fact that [27] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately. The evaluation and certification process might have taken place in advance or could – more likely – be carried out simultaneously to the current process according the PP in hand.

Application Note 1: There are separate Security Targets for BAC and EAC. Note, that the claim for conformance to the BAC-PP [27] does not require the conformance claim to the EAC-PP. Nevertheless claiming conformance of the (EAC-)PP [28] requires that the TOE meets a (separate) ST conforming to the BAC-PP [27].

For BAC, 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 [5], normative appendix 5.

The security target requires the TOE to implement the Chip Authentication defined in [29] and additionally the Active Authentication described in [5]. The Chip Authentication prevents data traces described in [5], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip

Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [29]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.2.4 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [26], the TOE life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (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 (ROM) 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.

Phase 2 "Manufacturing"

(Step3) 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 (ROM). 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.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

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

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

Application Note 2: Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF
- For JavaCard operating systems: the Applet instantiation.

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.

Phase 3 "Personalization of the MRTD"

(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [5] 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 3: The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the Chip Authentication Private Key.

Application note 4: This security target distinguishes 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 [5]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 4 "Operational Use"

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

Application note 5: 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 6: The intention of the PP is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the 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. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

Non-TOE hardware/software/firmware

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

2 Conformance Claim

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [4]

has to be taken into account.

2.2 PP Claim

This ST claims strict conformance to the Common Criteria Protection Profile – Machine Readable Travel Document with "ICAO Application", Extended Access Control [28].

Application note 7: Note that the Protection Profile [28] does not explicitly claim conformance to any other Protection Profile. Nevertheless, the TOE is required to fulfil the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' [27] as a premise to the Protection Profile [28].

2.3 Package Claim

This ST is conformant to the Assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in the CC, part 3 [3].

2.4 Conformance Claim Rationale

Since this ST is not claiming conformance to any other protection profile, no rationale is necessary here.

3 Security Problem Definition

This chapter corresponds to chapter 3 in the protection profile [28]. Minor additions have been performed covering the Active Authentication mechanism, which is indicated by underlined and bold text.

3.1 Introduction

3.1.1 Assets

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

Logical MRTD sensitive User Data

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

Application note 8: Due to interoperability reasons the 'ICAO Doc 9303' [5] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [27]).

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip

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

3.1.2 Subjects and external entities

This security target considers the following subjects:

Manufacturer
The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

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 [5].

Country Verifying Certification Authority
The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this

PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier
The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

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

Inspection system (IS)
A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (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. Optionally, the BIS may support Active Authentication. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

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

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

Attacker
A threat agent trying (i) to manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD.

Application note 9: Note that an attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this ST since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [27]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 as well as EF.SOD and EF.COM.

Application note 10: 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.

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

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

A.MRTD_Delivery MRTD delivery during steps 4 to 6

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

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

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, (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip), and (v) the Active Authentication Public Key (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object.

The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection Systems for global interoperability

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

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports 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.

A.Signature_PKI PKI for Passive Authentication

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

A.Auth_PKI PKI for Inspection Systems

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their MRTD's chip.

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.

Application note 11: The threats T.Chip_ID and T.Skimming (cf. [27]) are averted by the mechanisms described in the BAC PP [27] (cf. P.BAC-PP) which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

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

T.Read_Sensitive_Data Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [27]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and

therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

Threat agent: having high attack potential, knowing the Document Basic Access Keys, being in possession of a legitimate MRTD

Asset: confidentiality of sensitive logical MRTD (i.e. biometric reference) data

T.Forgery Forgery of data on MRTD's chip

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

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

Asset: authenticity of logical MRTD data

T.Counterfeit MRTD's chip

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

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

Asset: authenticity of logical MRTD data

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in "Operational Use" phase 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 high attack potential, being in possession of a legitimate MRTD

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

T.Information_Leakage Information Leakage from MRTD's chip

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

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

Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper Physical Tampering

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data

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

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

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

T.Malfunction Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

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

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

3.4 Organisational 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 [1], sec. 3.2).

P.BAC-PP Fulfilment of the Basic Access Control Protection Profile

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [5] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [27] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application note 12: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [5] is addressed by the [27] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [27]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed in separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also to Application Note 1).

P.Sensitive_Data Privacy of sensitive biometric reference data

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the MRTD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRTD is presented to the inspection system (Extended Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRTD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

P.Manufact Manufacturing of the MRTD's chip

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

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

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [5] 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 13: The OT.AC_Pers implies that

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

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

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 the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

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).

OT.Chip_Auth_Proof Proof of MRTD's chip authenticity

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [29]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

Application note 14: The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [5] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

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

OT.Prot_Abuse-Func Protection against Abuse of Functionality

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

OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip 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 15: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with 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.

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 16: 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.

OT.Active_Auth_Proof Proof of MRTD's chip authenticity

The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [5]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

4.2 Security Objectives for Operational Environment

Issuing State or Organization

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

OE.MRTD_Manufact Protection of the MRTD Manufacturing

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

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

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.

OE.Personalization Personalization of logical MRTD

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

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [5].

OE.Auth_Key_MRTD MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRTD's holders to authorized receiving States or Organizations. The Country Verifying Certification Authority of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.BAC_PP Fulfilment of the Basic Access Control Protection Profile

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' [27]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

OE.Active_Auth_Key_MRTD MRTD Active Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

Receiving State or Organization

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

OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing 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 [5]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveller 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.

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 inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

Application note 17: The figure 2.1 in [29] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication Protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence

has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this ST. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical MRTD. The Extended Inspection System authenticates themselves to the MRTD's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_Proof	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.BAC-PP	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_Systems	OE.Active_Auth_Key_MRTD
T.Read_Sensitive_Data			x													x					x	
T.Forgery	x	x						x						x				x	x			
T.Counterfeit					x					x					x			x				x
T.Abuse-Func						x																
T.Information_Leakage							x															
T.Phys-Tamper								x														
T.Malfunction									x													
P.BAC-PP																	x					
P.Sensitive_Data			x													x					x	
P.Manufact				x																		
P.Personalization	x			x									x									
A.MRTD_Manufact											x											
A.MRTD_Delivery												x										
A.Pers_Agent													x									
A.Insp_Sys																		x		x		
A.Signature_PKI														x				x				
A.Auth_PKI																x					x	

Table 1 Security Objective Rationale

The OSP **P.BAC-PP** is directly addressed by the **OE.BAC_PP**.

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 the management of TSF to the Personalization Agent.

The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems".

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.Counterfeit** "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRTD's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Exam_MRTD** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

Additionally, this attack is thwarted through the chip by an identification and authenticity proof required by **OT.Active_Auth_Proof** "Proof of MRTD's chip authentication" using an authentication key pair to be generated by the issuing state or organisation. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_MRTD** "MRTD Authentication Key".

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the "Operational Use" phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered.

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_Manufact** "MRTD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_Manufact** "Protection of the MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

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

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" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.Signature_PKI** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" covering the necessary procedures for the Country

Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD** "Examination of the MRTD passport book".

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organization has to establish the necessary public key infrastructure.

5 Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [24] other components are defined in the protection profile [28].

5.1 Definition of the Family FAU_SAS

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

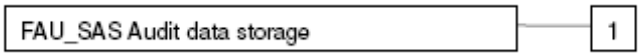
The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

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

Component levelling



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: *authorised users*] with the capability to store [assignment: *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 family (FCS_RND) of the class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

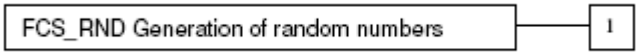
The family 'Generation of random numbers (FCS_RND)' is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:



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 FIA_API

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

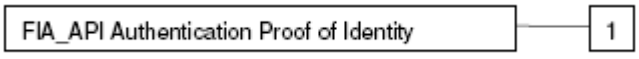
Application note 18: Other families of the class FIA describe only the authentication verification of user's identity performed by the TOE and do not describe the functionality of the TOE to prove its own identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Extended components definition (APE_ECD)') from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

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

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

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

5.4 Definition of the Family FMT_LIM

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

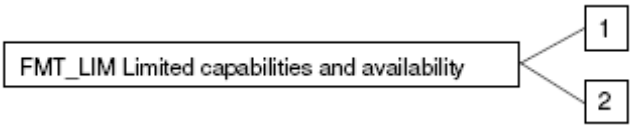
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



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*].

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

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

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both the requirements shall enforce the related policy.

5.5 Definition of the Family FPT_EMSEC

The family FPT_EMSEC (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against 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 being not directly addressed by any other component of CC part 2 [2].

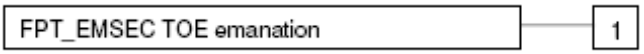
The family 'TOE Emanation (FPT_EMSEC)' is specified as follows:

FPT_EMSEC TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



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 [assignment: specified limits] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Requirements

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [1] of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments filled in by the ST author are denoted as double underlined text. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like *this*.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [2]. The operation "load" is synonymous to "import" used in [2].

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [29], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [29], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA

	DV (foreign)	roles defined in the certificate used for authentication (cf. [29], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [29], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [29], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [29], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [29], A.5.1)

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

Name	**Data**
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [29] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security

Name	Data
	attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys (K_{ENC} and K_{MAC})	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.
Active Authentication Key Pair	The Active Authentication Key Pair (KPr_{AA}, KPu_{IAA}) is used for the Active Authentication mechanism according to [5].
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment. A hash representation of DG15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D).
Active Authentication Private	The Active Authentication Private Key (KPr_{AA}) is used

Name	Data
Key (KPr_{AA})	by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.

Application note 20: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.1 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.

6.1.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[3] with the capability to store the IC Identification Data[4] in the audit records.

Application note 21: 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.1.1/INI_DIS).

6.1.2 Class FCS Cryptographic Support

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

FCS_CKM.1 Cryptographic key generation

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 ECDH compliant to ISO 15946[5,6] and

[3] [assignment: *authorised users*]

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

[5] [selection: *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946*]

specified cryptographic key sizes 112 bits[7], 192 bits – 521 bits[8,9] that meet the following: ISO/IEC14888-3 [8][10].

Application Note 22: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [29], sec. 3.1 and Annex A.1. This protocol is based on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [29], Annex A.1, [30] and [11] for details). The shared secret value is used to derive Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [5], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.

Application Note 22a: The TOE uses the following ECC brainpool curves: P224r1, P256r1, P320r1, see chapter 1.3.2 [30a] and NIST curves: P-256 (secp256r1), P-384 (secp384r1) and P-521 (secp521r1), see [30b].

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

FCS_CKM.4 Cryptographic key destruction

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 overwriting the key value with zero values[11] that meets the following: none[12].

Application Note 23: The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

6.1.2.1 Cryptographic operation (FCS_COP.1)

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

FCS_COP.1/SHA Cryptographic operation – Hash for key derivation by 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

[6] [assignment: *cryptographic key generation algorithm*]

[7] Bit length of 2-key Triple DES session keys

[8] Bit length of the curve

[9] [assignment*: cryptographic key sizes*]

[10] [assignment: *list of standards*]

[11] [assignment: *cryptographic key destruction method*]

[12] [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA The TSF shall perform hashing[13] in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512[14,15] and cryptographic key sizes none[16] that meet the following: FIPS 180-2 [23], Chapter 6[17,18].

Application Note 24: The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [5], annex E.1, cf. [27] also). The Chip Authentication Protocol may use SHA-1 (cf. [29], normative appendix 5, A5.1). The TOE implements additional hash functions SHA-224, and SHA-256 for the Terminal Authentication Protocol (cf. [29], Annex A.2.2 for details).

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

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/SYM The TSF shall perform secure messaging – encryption and decryption[19] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode, AES[20] and cryptographic key sizes 112 bits, 128 bits[21] that meet the following: FIPS PUB 46-3 [14], FIPS PUB 197 [13] Chapter 5[22].

Application Note 25: This SFR requires the TOE to implement the cryptographic primitives (Triple-DES and AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

Application Note 25a: This SFR requires the TOE to implement the cryptographic primitive AES during Personalization phase.

FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to: No other components.

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

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

[13] [assignment: *list of cryptographic operations*]

[14] [selection: *SHA-1, SHA-224, SHA-256 or other approved algorithms*]

[15] [assignment: *cryptographic algorithm*]

[16] [assignment: *cryptographic key sizes*]

[17] [assignment: *list of standards*]

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

[19] [assignment: *list of cryptographic operations*]

[20] [assignment: *cryptographic algorithm*]

[21] [assignment: *cryptographic key sizes*]

[22] [assignment: *list of standards*]

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[23] in accordance with a specified cryptographic algorithm Retail-MAC, CMAC[24] and cryptographic key sizes 112 bits, 128 bits[25] that meet the following: TR-03110 [29], Table A.1, EN14890 [22], Chapter 9.8.5[26].

Application Note 26: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over transmitted data. The key is agreed between the TSF by Chip Authentication Protocol according to the FCS_CKM.1. The Retail-MAC as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 (cf. [27]) is DES resp. two-key Triple-DES base.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification

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/SIG_VER The TSF shall perform digital signature verification[27] in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[28] and cryptographic key sizes 192-521 bits[29,30] that meet the following: ISO/IEC 14888-3 [8], Chapter 6.4[31].

Application Note 27: The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

Application Note 27a: The TOE uses the following ECC brainpool curves: P224r1, P256r1, P320r1, see chapter 1.3.2 [30a] and NIST curves: P-256 (secp256r1), P-384 (secp384r1) and P-521 (secp521r1), see [30b].

Application Note 27b: Padding is applied as described in Section 6.4.3.5 of ISO/IEC 14888-3 [8]. For example in case of SHA-512 hash function and P-521 curve, the hash-code H = h(M) of message M is converted to an integer according to the conversion rule BS2I given in Annex B of ISO14888-3.

FCS_COP.1/RSA_MRTD Cryptographic operation – Signature generation

Hierarchical to: No other components.

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

[23] [assignment: *list of cryptographic operations*]
[24] [assignment: *cryptographic algorithm*]
[25] [assignment: *cryptographic key sizes*]
[26] [assignment: *list of standards*]
[27] [assignment: *list of cryptographic operations*]
[28] [assignment: *cryptographic algorithm*]
[29] [assignment: *cryptographic key sizes*]
[30] Bit length of curve
[31] [assignment: *list of standards*]

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/RSA_MRTD The TSF shall perform digital signature generation[32] in accordance with a specified cryptographic algorithm RSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512[33] and cryptographic key sizes: 1024 bits–4096 bits[34] that meet the following: scheme 1 of ISO/IEC 9796-2:2002 [7], Chapter 8[35,36].

6.1.2.2 Random Number Generation (FCS_RND.1)

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

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet K4 (high) according to AIS20 [31][37].

Application Note 28: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.1.3 Class FIA Identification and Authentication

Application Note 29: The Table 2 provides an overview of the authentication mechanisms used.

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6
Terminal Authentication Protocol	FIA_UAU.5
Active Authentication Mechanism	FIA_API.1/AA

Table 2 Overview on authentication SFRs

Note the Chip Authentication Protocol as defined in this security target[38] includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [5] in order to gain access to the Chip Authentication Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,

[32] [assignment: *list of cryptographic operations*]

[33] [assignment: *cryptographic algorithm*]

[34] [assignment: *cryptographic key sizes*]

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

[36] According to [5], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.

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

[38] The BAC Authentication Protocol is included here as part of the Chip Authentication Protocol because it is a necessary condition to read the EF.DG14.

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

The BAC mechanism does not provide a security function on its own. The Chip Authentication Protocol may be used independent of the Terminal Authentication Protocol. But if the Terminal Authentication Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. to carry out the Chip Authentication Protocol[39]

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 30: In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The 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 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. PP MRTD BAC [27]) 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 run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this ST, it is a mandatory part within the Chip Authentication Protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).

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 establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,

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

3. to identify themselves by selection of the authentication key,
4. to carry out the Chip Authentication Protocol[40]

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.

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. Terminal Authentication Protocol,
2. Authentication Mechanism based on AES[41,42]

Application Note 31: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. Terminal Authentication Protocol,
2. Secure messaging MAC-ENC mode,
3. Symmetric Authentication Mechanism based on AES[43,44]

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 the Symmetric Authentication Mechanism with Personalization Agent Key[45].
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.

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

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

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

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

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

[45] [selection: *the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys*]

3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism.[46]

Application Note 32: Depending on the authentication methods used the Personalization Agent holds (i) a key for the Symmetric Authentication Mechanism or (ii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). 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 shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

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 after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS[47].

Application Note 33: The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [5] include 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 reauthenticates the user for each received command and accepts only those commands received from the previously authenticated user.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a Chip Authentication Protocol according to [29][48] to prove the identity of the TOE[49].

Application note 34: The TOE shall implement the Chip Authentication Mechanism specified in [29]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [5], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his

[46] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

[48] [assignment: *authentication mechanism*]

[49] [assignment: *authorized user or role*]

protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity – MRTD

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA The TSF shall provide the Active Authentication Mechanism according to [5][50] to prove the identity of the TOE[51].

6.1.4 Class FDP User Data Protection

FDP_ACC.1 Subset 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 Access Control SFP[52] 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[53].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the Access Control SFP[54] to objects based on the following:

1. Subjects:
   a. Personalization Agent,
   b. Extended Inspection System,
   c. Terminal,
2. Objects:
   a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
   b. data EF.DG3 and EF.DG4 of the logical MRTD
   c. data in EF.COM,
   d. data in EF.SOD
3. Security attributes:
   a. authentication status of terminals,
   b. Terminal Authorization[55]

[50] [assignment: *authentication mechanism*]

[51] [assignment: *authorized user or role*]

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

[53] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

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 Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.
3. the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD.[56]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[57].

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

1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD.[58]

Application Note 35: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [29], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Application Note 36: Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD. According to P.BAC-PP this security features of the MRTD are not subject of this security target.

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or

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

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

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

[58] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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 Access Control SFP[59] to be able to transmit and receive[60] user data in a manner protected from unauthorized disclosure **after Chip Authentication**.

FDP_UIT.1 Data exchange integrity

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 Access Control SFP[61] to be able to transmit and receive[62] user data in a manner protected from modification, deletion, insertion and replay[63] errors **after Chip Authentication**.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[64] has occurred **after Chip Authentication**.

Rationale for Refinement: Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [5] and [27]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [27]. The fact that the BAC mechanism is not part of the PP in hand is addressed by the refinement "after Chip Authentication".

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 Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.1.5 Class FMT Security Management

Application note 38: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements on the management of the TSF data.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

[59] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[60] [selection: *transmit, receive*]

[61] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[62] [selection: *transmit, receive*]

[63] [selection: *modification, deletion, insertion, replay*]

[64] [selection: *modification, deletion, insertion, replay*]

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[65]

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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. domestic Extended Inspection System,
6. foreign Extended Inspection System.[66]

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

Application note 39: Note that the MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. **OE.BAC_PP**. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

Application note 40: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced:
Deploying test features after TOE delivery do not allow

1. User Data to be manipulated,

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

[66] [assignment: *the authorised identified roles*]

2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed
3. TSF data to be disclosed or manipulated,
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.[67]

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced:
Deploying test features after TOE delivery do not allow

1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated,
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.[68]

Application note 41: The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note 42: 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.

FMT_MTD.1/INI_ENA Management of TSF data – Writing 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[69] the Initialization Data and Pre-personalization Data[70] to the Manufacturer[71].

[67] [assignment: *limited capability and availability policy*]

[68] [assignment: *limited capability and availability policy*]

[69] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[70] [assignment: *list of TSF data*]

[71] [assignment: *the authorised identified roles*]

Application note 43: 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.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization 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[72] the Initialization Data[73] to the Personalization Agent[74].

Application note 44: 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 restricts the ability to write the Initialization Data and the Pre-personalization Data by blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[75] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date[76]

to the Personalization Agent[77].

Application Note 45: The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent (cf. [29], sec. 2.2.6). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

[72] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[73] [assignment: *list of TSF data*]

[74] [assignment: *the authorised identified roles*]

[75] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]

[76] [assignment: *list of TSF data*]

[77] [assignment: *the authorised identified roles*]

FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update[78] the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[79]

to Country Verifying Certification Authority[80].

Application Note 46: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [29], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [29], sec. 2.2.3 and 2.2.4).

FMT_MTD.1/DATE Management of TSF data – Current date

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify[81] the Current date[82] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System[83].

Application Note 47: The authorized roles are identified in their certificate (cf. [29], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [29], annex A.3.3, for details).

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[84] the Document Basic Access Keys[85] to the Personalization Agent[86].

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

Application Note 48: The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *create, load*[87] the Chip Authentication Private Key[88] to the Manufacturer and the Personalization Agent[89].

Application note 49: The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Chip Authentication Private Key is generated by the TOE itself.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/AAPK The TSF shall restrict the ability to create, load[90] the Active Authentication Private Key[91] to the Manufacturer and the Personalization Agent[92].

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[93] the

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. Personalization Agent Keys
4. Active Authentication Private Key[94]

to none[95].

FMT_MTD.1/KEY_CHANGE Management of TSF data – Modification of Personalization Agent Key

[87] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[88] [assignment: *list of TSF data*]
[89] [assignment: *the authorised identified roles*]
[90] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[91] [assignment: *list of TSF data*]
[92] [assignment: *the authorised identified roles*]
[93] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[94] [assignment: *list of TSF data*]
[95] [assignment: *the authorised identified roles*]

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_CHANGE The TSF shall restrict the ability to modify[96] the Personalization Agent Key[97] to the Personalization Agent[98].

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2):

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control[99].

Refinement: The certificate chain is valid if and only if

(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

(2) the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

Application note 50: The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

6.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent

[96] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[97] [assignment: *list of TSF data*]
[98] [assignment: *the authorised identified roles*]
[99] [assignment: *list of TSF data*]

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.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit information about IC power consumption and command execution time[100] in excess of non useful information[101] enabling access to Personalization Agent Key(s) and Chip Authentication Private Key[102] and logical MRTD data and Active Authentication Private Key[103].

FPT_EMSEC.1.2 The TSF shall ensure any users[104] are unable to use the following interface smart card circuit contacts[105] to gain access to Personalization Agent Key(s) and Chip Authentication Private Key[106] and logical MRTD data and Active Authentication Private Key[107].

Application note 51: 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).

FPT_FLS.1/Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

[100] [assignment: *types of emissions*]
[101] [assignment: *specified limits*]
[102] [assignment: *type of users*]
[103] [assignment: *list of types of user data*]
[104] [assignment: *type of users*]
[105] [assignment: *type of connection*]
[106] [assignment: *type of users*]
[107] [assignment: *list of types of user data*]

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1[108]

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition[109] Reset of the TOE[110] to demonstrate the correct operation of the TSF[111].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[112].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application note 52: The MRTD's chip uses state of the art smart card technology and runs some self tests at the request of the authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the "authorized user" Manufacturer in the Phase 2 "Manufacturing". Other self tests are executed automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use", e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks.

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[113] to the TSF[114] by responding automatically such that the SFRs are always enforced.

Application note 53: The TOE shall 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.

[108] [assignment: *list of types of failures in the TSF*]

[109] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*]

[110] [assignment: *conditions under which self test should occur*]

[111] [selection: [assignment: *parts of TSF*], *the TSF*]

[112] [selection: [assignment: *parts of TSF*], *TSF data*]

[113] [assignment: *physical tampering scenarios*]

[114] [assignment: *list of TSF devices/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 54: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.2 Security Assurance Requirements for the TOE

The 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 the following components:

ALC_DVS.2 and AVA_VAN.5.

Application note 55: The TOE shall protect the assets against high attack potential under the assumption that the inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol (OE.Prot_Logical_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least Enhanced-Basic attack potential (AVA_VAN.3).

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
FAU_SAS.1				x						
FCS_CKM.1	x	x	x		x					
FCS_CKM.4	x	x	x							
FCS_COP.1/SHA	x	x	x		x					
FCS_COP.1/SYM	x	x	x		x					
FCS_COP.1/MAC	x	x	x		x					
FCS_COP.1/SIG_VER	x		x							
FCS_COP.1/RSA_MRTD	x	x	x							x
FCS_RND.1	x		x							
FIA_UID.1	x	x	x							

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
FIA_UAU.1	x	x	x							
FIA_UAU.4	x	x	x							
FIA_UAU.5	x	x	x							
FIA_UAU.6	x	x	x							
FIA_API.1					x					
FIA_API.1/AA										x
FDP_ACC.1	x	x	x							
FDP_ACF.1	x	x	x							
FDP_UCT.1			x							
FDP_UIT.1		x								
FMT_SMF.1	x	x								
FMT_SMR.1	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/CVCA_INI			x							
FMT_MTD.1/CVCA_UPD			x							
FMT_MTD.1/DATE			x							
FMT_MTD.1/KEY_WRITE	x									
FMT_MTD.1/CAPK		x	x		x					
FMT_MTD.1/AAPK		x	x							x
FMT_MTD.1/KEY_READ	x	x	x		x					x
FMT_MTD.1/KEY_CHANGE	x									
FMT_MTD.3			x							
FPT_EMSEC.1	x						x			
FPT_TST.1							x		x	
FPT_FLS.1							x		x	
FPT_PHP.3							x	x		

Table 3 Coverage of 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 FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: 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 SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The

Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMSEC.1 the confidentially of these keys.

The TOE allows changing Personalization Agent Keys by the Personalization Agent according to the SFR FMT_MTD.1/KEY_CHANGE.

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 in 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 in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6. The SFR FIA_UAU.6 and FDP_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1 (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1.1/CAPK and FMT_MTD.1.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The SFR FIA_UID.1 and FIA_UAU.1 requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4. The SFR FIA_UAU.6 and FDP_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1 (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The

session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1.1/CAPK and FMT_MTD.1.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The security objective **OT.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.

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 security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1 is performed using a TOE internally stored confidential private key as required by FMT_MTD.1.1/CAPK and FMT_MTD.1.1/KEY_READ. The Chip Authentication Protocol [29] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

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.

The security objective **OT.Active_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Active Authentication Protocol provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by

FMT_MTD.1/AAPK and FMT_MTD.1.1/KEY_READ. The Active Authentication Protocol [5] requires additional TSF according to FCS_COP.1/RSA_MRTD.

6.3.2 Dependency Rationale

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

The Table 4 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/SYM, 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/SYM	[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/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_COP.1/SIG_VER	[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/RSA_MRTD	[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 A for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 2 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	justification 3 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/CVCA_INI	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/CVCA_UPD	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/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
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_CHANGE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
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 4 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 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. 3: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

No. 4: The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

No. A: The SFR FCS_COP.1/RSA_MRTD does not calculate any shared secrets, nor does it import user data. Therefore there is no need for any special security attributes.

6.3.3 Security Assurance Requirements Rationale

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

The 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 MRTD's material.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

All of these are met or exceeded in the EAL4 assurance package.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and

the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

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

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

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

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

6.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Infineon derivates SLE78CLX360P, SLE78CLX800P, SLE78CLX1280P [33]. This statement is compliant to the requirements of [4a].

6.4.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functionality	Relevant	Not relevant
SF_DPM: Device Phase Management	x	
SF_PS: Protection against Snooping	x	
SF_PMA: Protection against Modifying Attacks	x	
SF_PLA: Protection against Logical Attacks	x	
SF_CS: Cryptographic Support	x	

Table 5 Classification of Platform-TSFs

All listed TSFs of the Platform-ST are relevant for the Composite-ST.

6.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon microcontroller derivates SLE78CLX360P, SLE78CLX800P, SLE78CLX1280P; the optional RSA2048/4096 v1.02.008, EC v1.02.008 and SHA-2 v1.01 libraries are not used by the composite TOE,
- True Random Number Generator (TRNG) with P2 classification according to AIS31 [32].
- Cryptographic support based on asymmetric and symmetric key algorithms (RSA, ECDSA, AES, Triple-DES) with 1024-4096 bits (RSA modulus) and 192-521 bits (elliptic curve) asymmetric key length, 128 bits (AES) and 112 bits (2-key Triple-DES) symmetric cryptographic key length.

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

6.4.2.1 TOE Security Environment

6.4.2.1.1 Threats and OSPs

(see chapters 3.3 Threats and 3.4 Organisational Security Policies)

None of the OSPs of the Composite-ST are applicable to the IC and therefore not mapable for the Platform-ST.

The augmented organizational security policy P.Add-Functions of the Platform-ST deals with additional specific security components like the AES encryption and decryption and could therefore be mapped to OT.Prot_Inf_Leak and OT.Prot_Phys-Tamper of the Composite-ST.

The following threats of this Composite-ST are directly related to IC functionality:

- T.Phys-Tamper
- T.Malfunction
- T.Abuse-Func
- T.Information_Leakage
- T.Forgery

These threats will be mapped to the following Platform-ST threats:

- T.Leak-Inherent
- T.Phys_Probing
- T.Malfunction
- T.Phys_Manipulation
- T.Leak-Forced
- T.Abuse-Func
- T.RND
- T.Mem-Access

The following table shows the mapping of the threats.

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced	T.Abuse-Func	T.RND	T.Mem-Access
Composite-ST	T.Phys_Tamper	x	x	x	x	x		x	
	T.Malfunction				x				
	T.Abuse-Func						x		x
	T.Information_Leakage	x	x	x	x	x	x		
	T.Forgery			x	x				

Table 6 Mapping of threats

T.Phys-Tamper matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.RND as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

T.Abuse-Func matches to T.Mem-Access as security violations either accidentally or deliberately could access restricted data (which may include code) or privilege levels.

T.Information_Leakage matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.Abuse-Func as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data.

T.Forgery matches to T.Phys_Manipulation and T.Malfunction because if an attacker fraudulently alters the User Data or/and TSF-data stored on the MRTD or/and exchanged between the TOE and the inspection system then the listed threats of the Platform-ST could be relevant.

6.4.2.1.2 Assumptions

The assumptions from this ST (see chapter 3.2 Assumptions) make no assumptions on the Platform.

The assumptions from the Platform-ST [33] are as follows:

Assumption	Classification of assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC	not relevant	n/a
A.Plat-Appl	not relevant	n/a
A.Resp-Appl	relevant	OT.Data_Int, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper
A.Key-Function	relevant	OT.Prot_Inf_Leak

Table 7 Mapping of assumptions

There is no conflict between security environments of this Composite-ST and the Platform-ST [33].

6.4.2.2 Security objectives

This Composite-ST has security objectives which are related to the Platform-ST. These are:

- OT.Prot_Abuse-Func
- OT.Prot_Inf_Leak
- OT.Prot_Phys-Tamper
- OT.Identification
- OT.Prot_Malfunction

The following platform objectives could be mapped to composite objectives:

- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Abuse-Func
- O.Leak-Forced
- O.Leak-Inherent
- O.Identification

These Platform-ST objectives can be mapped to the Composite-ST objectives as shown in the following table.

Platform-ST		O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification
Composite-ST	OT.Prot_Abuse-Func				x			
	OT.Prot_Inf_Leak					x	x	
	OT.Prot_Phys-Tamper	x	x	x				
	OT.Identification							x
	OT.Prot_Malfunction		x					

Table 8 Mapping of objectives

The following Platform-ST objectives are not relevant for or cannot be mapped to the Composite-TOE:

- O.Add-Functions cannot be mapped
- O.MEM_ACCESS is not relevant because the Composite-TOE does not use area based memory access control.

All Security Objectives for the Environment (see chapter 4.2 and [28]) are not linked to the platform and are therefore not applicable to this mapping. These objectives are:

- OE.MRTD_Manufact
- OE.MRTD_Delivery

- OE.Personalization
- OE.Pass_Auth_Sign
- OE.Auth_Key_MRTD
- OE.Authoriz_Sens_Data
- OE.BAC_PP
- OE.Passive_Auth_Verif
- OE.Prot_Logical_MRTD
- OE.Ext_Insp_Systems

There is no conflict between security objectives of this Composite-ST and the Platform-ST [33].

6.4.2.3 Security requirements

6.4.2.3.1 Security Functional Requirements

This Composite-ST has the following platform-related SFRs:

- FCS_CKM.1
- FCS_COP.1/MAC
- FCS_COP.1/SYM
- FCS_COP.1/SIG_VER
- FCS_COP.1/RSA_MRTD
- FCS_RND.1
- FPT_PHP.3
- FPT_EMSEC.1
- FPT_FLS.1
- FPT_TST.1
- FMT_LIM.1
- FMT_LIM.2
- FAU_SAS.1

The following Platform-SFRs could be mapped to Composite-SFRs:

- FCS_RNG.1
- FCS_COP.1/DES
- FCS_COP.1/AES
- FCS_COP.1/RSA
- FCS_COP.1/ECDSA
- FCS_CKM.1/EC
- FRU_FLT.2
- FPT_PHP.3

- FPT_FLS.1
- FPT_TST.2
- FMT_LIM.1/2
- FAU_SAS.1

They will be mapped as seen in the following table.

Platform-ST		FCS_RNG.1	FCS_COP.1/DES	FCS_COP.1/AES	FRU_FLT.2	FPT_FLS.1	FPT_PHP.3	FMT_LIM.1	FMT_LIM.2	FAU_SAS.1	FPT_TST.2	FCS_CKM.1/EC	FCS_COP.1/ECDSA	FCS_COP.1/RSA
Composite-ST	FCS_CKM.1											x		
	FCS_COP.1/MAC		x											
	FCS_COP.1/SYM		x	x										
	FCS_COP.1/SIG_VER												x	
	FCS_COP.1/RSA_MRTD													x
	FCS_RND.1	x												
	FPT_PHP.3				x	x	x							
	FPT_EMSEC.1						x							
	FPT_FLS.1					x								
	FPT_TST.1										x			
	FMT_LIM.1							x						
	FMT_LIM.2								x					
	FAU_SAS.1									x				

Table 9 Mapping of SFRs

FCS_COP.1/SYM and FCS_COP.1/MAC of the Composite-ST match FCS_COP.1/DES of the Platform-ST when the DES coprocessor is used by the TOE.

FCS_COP.1/SYM of the Composite-ST matches FCS_COP.1/AES of the Platform-ST when the AES coprocessor is used by the TOE.

FCS_CKM.1 of the Composite-ST matches to FCS_CMK.1/EC of the Platform-ST for cryptographic key generation.

FCS_COP.1/RSA_MRTD of the Composite-ST matches to FCS_COP.1/RSA of the Platform-ST when the Crypto2304T coprocessor is used by the TOE for digital signature generation.

FCS_COP.1/SIG_VER of the Composite-ST matches to FCS_COP.1/ECDSA of the Platform-ST when the Crypto2304T coprocessor is used by the TOE for digital signature verification.

FPT_PHP.3 of the Composite-ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform-ST.

FMT_LIM.1 and FMT_LIM.2 of the Composite-ST match to the equivalent SFR of the Platform-ST.

FAU_SAS.1 of the Composite-ST matches to the equivalent SFR of the Platform-ST.

The following Platform-SFRs are not mapped to Composite-SFRs:

- FCS_CKM.1/RSA, because the RSA key generation is not used by the TOE.
- FCS_COP.1/ECDH, because the TOE implements the ECDH key agreement according to [29], Annex A.1, that is covered by FCS_CKM.1 of the Composite-ST.
- FDP_ACC.1, because the composite TOE is always in system mode and therefore no MMU is necessary and because the composite TOE does not use the platform TOE special function registers.
- FDP_ACF.1, because the composite TOE does not use the platform TOE special function registers and the MMU.
- FMT_MSA.1, because the composite TOE is always in system mode and therefore no MMU and special function registers is necessary.
- FMT_MSA.3, because the composite TOE is always in system mode and therefore no MMU is necessary.
- FMT_SMF.1, because the TOE does not change the CPU mode.
- FDP_ITT.1, because it deals with the internal data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FPT_ITT.1, because it deals with the basic internal data protection of the platform TOE that does not by itself impact the composite TOE.
- FDP_IFC.1, because it deals with the data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FDP_SDI.1 and FDP_SDI.2 are not applicable to the composite TOE. Protection against malfunctions is covered by the SFRs FPT_TST.1 and FPT_FLS.1 of the composite TOE.

6.4.2.3.2 Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R3 augmented by ALC_DVS.2 and AVA_VAN.5.

The Platform-ST requires EAL 5 according to Common Criteria V3.1 R3 augmented by: ALC_DVS.2 and AVA_VAN.5.

As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of the Composite-ST will match to the Platform-ST assurance requirements.

6.4.3 Overall no contradictions found

Overall there is **no conflict** between **security requirements** of this Composite-ST and the Platform-ST.

7 TOE summary specification

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

7.1 TOE Security Functions

7.1.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users (Manufacturer, Personalization Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), domestic Extended Inspection System, foreign Extended Inspection System).

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

Personalization Agent is the only role with the ability:

- to disable read access for users to the Initialization Data.
- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date.
- to write the Document Basic Access Keys.
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD after successful authentication.

The access control mechanisms ensure that only the Country Verifying Certification Authority has the ability to update the CVCA Public Key and the CVCA Certificate.

The access control mechanisms ensure that only authenticated Extended Inspection System with the Read access to

- DG 3 (Fingerprint) is allowed to read the data in EF.DG3 of the logical MRTD.
- DG 4 (Iris) is allowed to read the data in EF.DG4 of the logical MRTD.

In all other cases, reading any of the EF.DG3 to EF.DG4 of the logical MRTD is explicitly denied.

The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys, the Chip Authentication Private Key, the Personalization Agent Keys, and the Active Authentication Private Key.

A terminal authenticated as CVCA or as DV is explicitly denied to read data in the EF.DG3 and EF.DG4.

Any terminal is explicitly denied to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.

Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.

Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be manipulated, sensitive User Data (EF.DG3 and EF.DG4) to be disclosed, 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 access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

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

7.1.2 SF_Authentication

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

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

The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [31] that provides random numbers used authentication. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying IC.

The TOE supports user authentication by the following means:

- Terminal Authentication Protocol
- Secure messaging in MAC-ENC mode
- Symmetric Authentication Mechanism

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

- Chip Authentication Protocol
- Active Authentication Mechanism

The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol
- Symmetric Authentication Mechanism

Personalization Agent authenticates himself to the TOE by use of the Personalization Agent Keys with the following symmetric cryptographic mechanisms:

- Symmetric Authentication Mechanism

After completion of the Chip Authentication Protocol, the TOE accepts commands with correct message authentication code only. These commands must have been sent via secure messaging using the key previously agreed with the terminal by means of the Chip Authentication Mechanism.

The TOE accepts terminal authentication attempts by means of the Terminal Authentication Protocol only via secure messaging that was established by the preceding Chip Authentication Protocol.

The TOE verifies each command received after successful completion of the Chip Authentication Protocol as having been sent by the GIS.

Protection of user data transmitted from the TOE to the terminal is achieved by means of secure messaging with encryption and message authentication codes after successful

Chip Authentication to the General Inspection System. After Chip Authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay errors.

7.1.3 SF_AssetProtection

The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as well as temporarily stored hash values for data to be signed.

The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

7.1.4 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

The TOE is resistant to physical tampering on the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

7.1.5 SF_KeyManagement

The TOE supports onboard generation of cryptographic keys based on the ECDH compliant to ISO 15946 [29], Annex A.1.

A successfully authenticated Personalization Agent is allowed to change the Personalization Agent Keys.

The TOE supports overwriting the cryptographic keys with zero values as follows:

- the BAC Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol,
- the Chip Session Keys after detection of an error in a received command by verification of the MAC,
- any session keys before starting the communication with the terminal in a new power-on-session.

7.1.6 SF_SignatureGeneration

The TOE supports digital signature creation by use of cryptographic algorithm RSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512, and cryptographic key sizes of 1024 bits – 4096 bits that meet scheme 1 of ISO/IEC 9796-2:2002 [7].

7.2 Assurance Measures

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

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

Assurance Measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.
AM_AGD	The guidance documentation is described in the operational user guidance documentation and in the documentation for preparative procedures.
AM_ALC	The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

Table 10 References of Assurance measures

7.3 Fulfilment of the SFRs

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

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration
FAU_SAS.1	x					
FCS_CKM.1					x	
FCS_CKM.4					x	
FCS_COP.1/SHA		x			x	
FCS_COP.1/SYM		x		x		
FCS_COP.1/MAC		x		x		
FCS_COP.1/SIG_VER		x		x		
FCS_COP.1/RSA_MRTD				x		x
FCS_RND.1		x		x		
FIA_UID.1		x				

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement	SF_SignatureGeneration
FIA_UAU.1		x				
FIA_UAU.4		x				
FIA_UAU.5		x				
FIA_UAU.6		x				
FIA_API.1		x				
FIA_API.1/AA		x				
FDP_ACC.1	x					
FDP_ACF.1	x					
FDP_UCT.1		x				
FDP_UIT.1		x				
FMT_SMF.1	x					
FMT_SMR.1	x					
FMT_LIM.1	x		x			
FMT_LIM.2	x		x			
FMT_MTD.1/INI_ENA	x					
FMT_MTD.1/INI_DIS	x					
FMT_MTD.1/CVCA_INI	x					
FMT_MTD.1/CVCA_UPD	x					
FMT_MTD.1/DATE	x					
FMT_MTD.1/KEY_WRITE	x					
FMT_MTD.1/CAPK	x					
FMT_MTD.1/AAPK	x					
FMT_MTD.1/KEY_READ	x					
FMT_MTD.1/KEY_CHANGE	x					
FMT_MTD.3	x					
FPT_EMSEC.1			x			
FPT_TST.1				x		
FPT_FLS.1				x		
FPT_PHP.3				x		

Table 11 Mapping of SFRs to mechanisms of TOE

7.3.1 Justifications for the correspondence between functional requirements and TOE mechanisms

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

7.4 Rationale for PP Claims

This security target is conformant to the claimed PP [28]. Additionally, the Active Authentication Mechanism is included in the TOE. This implies the below described augmentations.

Extension of TOE Asset:

- A.Pers_Agent: Personalization Agent to ensure the correctness of the Active Authentication Public Key

Addition of new TOE Objectives:

- OT.Active_Auth_Proof

Addition of new IT Environment Objectives:

- OE.Active_Auth_Key_MRTD

Addition of new SFRs for the TOE:

- FCS_COP.1/RSA_MRTD
- FIA_API.1/AA
- FMT_MTD.1/AAPK

Extension of existing SFRs for the TOE to include the Active Authentication private key:

- FMT_MTD.1.1/KEY_READ
- FPT_EMSEC.1.1 and FPT_EMSEC.1.2

In the personalization phase the TOE allows the Personalization Agent to use the EXTERNAL AUTHENTICATE command to replace the existing Personalization Agent keys. This implies the following augmentation:

Addition of new SFR for the TOE:

- FMT_MTD.1.1/KEY_CHANGE

8 Glossary and Acronyms

8.1 Glossary

Term	Definition
Active Authentication	Security mechanism defined in [5] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application Note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTD's chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Control Access (BAC)	Security mechanism defined in [5] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [5]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Terminal Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means. [5]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the

Term	Definition
	MRTD.
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.
Document Basic Access Key Derivation Algorithm	The [5], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [5]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}). [5]
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
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [5]
Extended Access Control	Security mechanism identified in [5] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control

Term	Definition
	Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait. [5]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all MRTDs. [5]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [5]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [5]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life cycle, Phase 2, Step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [5]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [5]
Issuing State	The country issuing the MRTD. [5]

Term	Definition
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [5]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16) (6) EF.COM and EF.SOD
Logical Travel Document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [5]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [5]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [5]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [5]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [5], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ

Term	Definition
	information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [6], p. 14.
MRTD's Chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.2, TOE life cycle, Phase 3, Step 6).
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. sec. 1.2, TOE life cycle, Phase 2, Step 5)
Pre-Personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between

Term	Definition
	life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the Traveler is applying for entry. [5]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [5]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organisation which may be used by the rightful holder for international travel. [5]
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User Data	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [5]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

8.2 Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File
EIS	Extended Inspection System

Acronym	Term
GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number
MF	Master File
n.a.	Not applicable
OSP	Organisational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functionality

9 Bibliography

9.1 Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[4a] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-007-09-001

9.2 ICAO

[5] ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, volume 2, ICAO, 6th edition, 2006

[6] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

9.3 Cryptography

[7] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

[8] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[9] ISO/IEC 15946-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[10] ISO/IEC 15946-2: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[11] ISO/IEC 15946-3: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[12] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993

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

[14] Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[15] Federal Information Processing Standards Publication FIPS PUB 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[16] Federal Information Processing Standards Publication FIPS PUB 180-2 Secure Hash Standard (and Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002

[17] NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999

[18] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, May 2005

[19] ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996

[20] ANSI X9.62-1999, AMERICAN NATIONAL STANDARD, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[21] Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006

[22] CEN/TC 224, EN 14890-1 Application Interface for smart cards used as Secure Signature Creation Devices — Part 1: Basic services

[23] Federal Information Processing Standards Publication 180-2 (+Change Notice to include SHA-224), 2002 August 1, Specifications for the SECURE HASH STANDARD

9.4 Protection Profiles

[24] Common Criteria Protection Profile PP conformant to Smartcard IC Platform, BSI-PP-0002-2001, version 1.0, July 2001

[25] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[26] Common Criteria Protection Profile Security IC Platform, BSI-PP-0035-2007, version 1.0, June 2007

[27] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, version 1.10, 25th March 2009

[28] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, version 1.10, 25th March 2009

9.5 Technical Guidelines and Directives

[29] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[30] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[30a] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Stand 2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[30b] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection establishment (PACE), and restricted Identification (RI), Version 2.05, 14.10.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[31] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 02.12.1999

[32] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

9.6 Other

[33] Security Target, Infineon, M7820 A11, Version 1.5, 07.05.2012

[34] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2000

[35] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[36] STARCOS 3.5 ID TABLES, Giesecke & Devrient

[37] Generic MRTD Application Verifier Tool for STARCOS 3.5 ID, Version 4.0, 28.03.2012, Giesecke & Devrient