Security Target – lite –

Machine Readable Travel Document with "ICAO Application", Extended Access Control MTCOS Pro 2.1 EAC/P5CD080/V2

MASKTECH INTERNATIONAL GMBH

Document number: BSI-DSZ-CC-0658, ST, Version 1.1

Created by: Gudrun Schürer

Date: 2010-07-12

Signature:

Released by Management:

Date:

Signature:

Change history

Version	Date	Reason	Remarks
1.0	2010-04-16	First version based on the Security Target of BSI-DSZ-CC-0658	
1.1	2010-07-12	References updated	

Contents

1 ST Introduction **5**

1.1 ST Reference 5

1.2 ST Overview 5

1.3 Conformance Claim 6

2 TOE Description **7**

2.1 TOE definition 7

2.1.1 TOE Usage and Security Features for Operational Use 7

2.2 TOE Life Cycle 9

2.3 Use of TOE 11

2.4 Limits of the TOE 11

2.4.1 Architecture 11

3 Security Problem Definition **12**

3.1 Introduction 12

3.2 Assumptions 14

3.3 Threats 15

3.4 Organizational Security Policies 18

3.5 Security Objectives 19

3.5.1 Security Objectives for the TOE 19

3.5.2 Security Objectives for the Development and Manufacturing Environment 21

3.5.3 Security Objectives for the Operational Environment 22

4 Security Requirements **24**

4.1 Security Functional Requirements for the TOE 26

4.1.1 Class FAU Security Audit 26

4.1.2 Class Cryptographic Support (FCS) 26

4.1.3 Class FIA Identification and Authentication 30

4.1.4 Class FDP User Data Protection 35

4.1.5 Class FMT Security Management . . . 38
4.1.6 Class FPT Protection of Security Functions . . . 43
4.2 Security Assurance Requirements for the TOE . . . 45
4.3 Security Requirements for the IT Environment . . . 46
4.3.1 Passive Authentication . . . 46
4.3.2 Extended Access Control PKI . . . 46
4.3.3 Basic Terminal . . . 48
4.3.4 General Inspection System . . . 51
4.3.5 Extended Inspection System . . . 55
4.3.6 Personalization Terminals . . . 56

5 TOE Summary Specification 58
5.1 TOE Security Functions . . . 58
5.1.1 TOE Security Functions from Hardware (IC) and Crypto Library . . . 58
5.1.2 TOE Security Functions from Embedded Software (ES) – Operating system . . . 59
5.2 Assurance Measures . . . 63

6 PP Claims 64
6.1 PP Reference . . . 64
6.2 PP Refinements . . . 64
6.3 PP Additions . . . 64

7 Rationale 65
7.1 Security Objectives Rationale . . . 65
7.2 Security Requirements Rationale . . . 69
7.2.1 Security Functional Requirements Rationale . . . 69
7.2.2 TOE Summary Specification Rationale . . . 78
7.2.3 Rationale for Assurance Measures . . . 83
7.2.4 Security Assurance Requirements Rationale . . . 83
7.2.5 Security Requirements – Mutual Support and Internal Consistency . . . 84
7.2.6 Strength of Function Level Rationale . . . 85
7.3 Rationale for PP Claims . . . 85
7.4 Statement of Compatibility . . . 86
7.4.1 Relevance of Hardware TSFs . . . 86
7.4.2 Compatibility: TOE Security Environment . . . 87
7.4.3 Conclusion . . . 97

8 Glossary and Acronyms **98**

Chapter 1

ST Introduction

1.1 ST Reference

Title	Security Target – lite – Machine Readable Travel Document with ICAO Application, Extended Access Control, V2 (ST-MRTD EAC V2)
Version	1.1, 2010-07-12
Editors	Gudrun Schürer
PP used	Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.2, BSI-PP-0026
Assurance Level	The level for this ST is EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
Hardware	NXP P5CD080V0B [1]
TOE version	MTCOS Pro 2.1 EAC
Keywords	ICAO, machine readable travel document, extended access control

1.2 ST 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, Active Authentication, Extended Access Control and chip authentication similar to the Active Authentication in the Technical reports of the ICAO New Technology Working Group.

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816. It provides public and secret key cryptography and supports also other applications like e-purses, health insurance cards and access control.

The operating system software is implemented on the NXP P5CD080V0B secure dual-interface controller with the Secured Crypto Library, which is certified according to CC EAL5 augmented (BSI-DSZ-CC-0417). This means, that the TOE consists of software and hardware.

The assurance level for the TOE is CC EAL4 augmented.

The minimum strength level (SOF) for the TOE security functions is high.

1.3 Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005, CCMB-2005-08-003

as follows

- Part 2 extended
- Part 3 conformant
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

Chapter 2

TOE Description

2.1 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) [2] and providing the Basic Access Control, the Active Authentication, the Extended Access Control according to the ICAO document[3] and the chip authentication according to the technical report TR-03110 [4].

The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors
- 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
- the associated guidance documentation [5, 6, 7, 8, 9]

2.1.1 TOE Usage and Security Features for Operational Use

State or organization issues MRTD 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 [2] 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

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)
3. the printed portrait

the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [2] as specified by ICAO on the contactless integrated circuit. It presents over the logical interface of APDUs 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
4. the other data according to LDS (EF.DG5 to EF.DG16)
5. the Document Security Object

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [10]. 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 Technical report [3]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism. This security target addresses the Chip Authentication described in [4] as an alternative or as an addition to the Active Authentication stated in [3].

The Basic Access Control is a security feature that shall be mandatory implemented by the TOE. The Inspection System (i) reads optically the MRTD, (ii) authenticates itself as Inspection System by means of Document Basic Access Keys. After successful authentication of

the Inspection System the MRTD's chip provides read access to the logical MRTD by means of private communication (Secure Messaging) with this Inspection System according to [3], Annex E, and [2].

The security target requires the TOE to implement the Chip Authentication defined in [4] and the Active Authentication described in [3]. Both protocols provide evidence of the MRTD's chip authenticity where the Chip Authentication prevents data traces described in [3], Annex G, section G.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 a 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. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key 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 [4]. The Extended Access Control consists of two parts (i) a Terminal Authentication Protocol to authenticate the Inspection System as entity authorized by the Issuing State or Organization through the receiving State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized Inspection Systems. It requires the Chip Authentication of the MRTD's chip to the Inspection System and uses the Secure Messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the Inspection System. 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.

2.2 TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases.

Development 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.

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.

Manufacturing 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 nonprogrammable 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 manufacture to the MRTD manufacturer.

The MRTD manufacturer (i) adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, (iii) equips MRTD's chips with pre-personalization Data, and (iv) combines the IC with hardware for the contactless interface in the passport book.

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.

For easier handling this phase is split into:

1. IC manufacturing: Manufacturing of the chip including Identification Data by the IC manufacturer.
2. Wafer fab: The MRTD manufacturer loads the image of the basic filesystem and the patch generated on the emulator as well as the derives keys and the Project ID into the EEPROM.
3. Initialization and Pre-personalization: The MRTD manufacturer generates the MRTD application and prepares the TOE for the personalization, e.g. creates of data files.

Personalization of the MRTD The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrollment 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) the writing of the TSF Data into the logical MRTD and 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 [3] 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.

Operational Use 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.

2.3 Use of TOE

The TOE is implemented as a smart card IC, which supports the communication via a contactless interface according to ISO/IEC 14443 [11]. It is based on ISO/IEC 7816 [12] commands and is intended to be used inside a MRTD as storage of the digital data and supports Basic Access Control and Extended Access Control.

Because of the support of ISO/IEC 7816 the TOE can be also used as multi-application smart card with applications of health care, e-purse or loyalty.

2.4 Limits of the TOE

2.4.1 Architecture

The TOE is an RFID device according to ICAO technical reports [2] and [3] supporting Basic and Extended Access Control. It is implemented as an embedded software on a smart card chip, in this case the CC EAL 5+ certified NXP P5CD080V0B. The TOE is the MTCOS Pro smart card operating system stored in the ROM of the IC, the file system including application data, any configurable and non-volatile parameters and perhaps parts of the operating system stored in EEPROM and the IC itself.

The TOE provides following services for MRTDs:

- Storage of the MRTD data, e.g. data groups and signature
- Organization of the data in a file system as dedicated and elementary files
- Mutual Authenticate and Secure Messaging as specified in TrPKI [3] for Basic Access Control
- Extended Access Control (EAC) as specified in TR-03110 [4]
- Active Authentication as specified in TrPKI [3]
- Contactless communication according to ISO/IEC 14443 [11]
- Protection of the privacy of the passport holder with functions like random UID and Basic Access Control

The TOE life cycle is as defined in the preceding subsection with the addition, that the operating system distinguishes in Phase 2 between initialization mode and operational mode. In initialization mode the operating system can be configured with Secure Messaging protected commands. In this phase also the file system is created. The pre-personalization is done in Phase 2 after switching the OS to operational mode. The operating system is in the operational mode until end of life.

Chapter 3

Security Problem Definition

3.1 Introduction

Assets

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

Logical MRTD Data The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [2]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) is used by the Inspection System for the Chip Authentication and the Active Authentication Public Key (EF.DG15) for Active Authentication. The EF.SOD is used by the Inspection System for Passive Authentication of the logical MRTD.

User Data	**TSF Data**
Personal Data of the MRTD holder (EF.DG1, EF.DG2,	Personalization Agent
EF.DG5 - EF.DG13, EF.DG15, EF.DG16)	Reference Authentication Data
Sensitive biometric reference data (EF.DG3, EF.DG4)	Basic Access Control (BAC) Key
Chip Authentication Public Key in EF.DG14	Public Key CVCA
Active Authentication Public Key in EF.DG15	Active Authentication Private Key
Document Security Object (SOD) in EF.SOD	CVCA Certificate
Common data in EF.COM	Current date
	Chip Authentication Private Key

Table 3.1: Assignment of User and TSF Data

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 proof his possession of a genuine MRTD.

Subjects

This security target considers the following subjects:

Manufacturer The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 *Manufacturing*. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer. During pre-personalization the MRTD manufacturer (so-called Pre-Personalization Agent) prepares the TOE for the personalization, e.g. creation of data files.

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 [2].

Country Verifying Certification Authority The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing Country 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 form of Country Verifying CA Link-Certificates.

Document Verifier The Document Verifier (DV) enforces the privacy policy of the receiving Country 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 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. The General Inspection System (GIS) is a Basic Inspection System which implements additional 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. Optionally all the Inspection Systems can implement Active Authentication.

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

Traveler Person presenting the MRTD to the Inspection System and claiming the identity of the MRTD holder.

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

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.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) and Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection (Systems for global interoperability) The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the

terminal part of the Basic Access Control [3]. The Basic Inspection System reads the logical MRTD being 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. Optionally all the Inspection Systems can implement Active Authentication.

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 (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the MRTD's Chip Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes 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 and distributes them 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 distributes the public key 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.

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

T.Chip_ID (Identification of MRTD's chip) An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker cannot read optically and does not know in advance the physical MRTD.

T.Skimming (Skimming the logical MRTD) An attacker imitates the Inspection System to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know in advance the physical MRTD.

T.Read_Sensitive_Data (Read the sensitive biometric reference data) An attacker with high attack potential knowing the Document Basic Access Keys is trying 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 threats T.Skimming 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 visual readable on the physical MRTD as well.

T.Forgery (Forgery of data on MRTD's chip) An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose 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 write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveler into an other 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 in another contactless chip.

T.Counterfeit (MRTD's chip) 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.

The TOE shall avert the threat as specified below.

T.Abuse-Func (Abuse of Functionality) An attacker may use functions of the TOE which shall not be used in TOE operational 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.

T.Information_Leakage (Information Leakage from MRTD's chip) 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).

T.Phys-Tamper (Physical Tampering) 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.

T.Malfunction (Malfunction due to Environmental Stress) 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.

3.4 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2 [13]).

P.Manufact (Manufacturing of the MRTD's chip) The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 *Manufacturing*. The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

P.Personal_Data (Personal data protection policy) The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an Inspection System. Additional to the Basic Access Control Authentication defined by ICAO in [3] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

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. 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.

3.5 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.

3.5.1 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 [2] 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.

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.Data_Conf (Confidentiality of personal data) The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as (i) Personalization Agent or (ii) Basic Inspection System or (iii) Extended Inspection System. The TOE implements the Basic Access Control as defined by ICAO [3] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the 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 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 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*. In Phase 4 *Operational Use*, the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

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 [4]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

Security Objectives independent on the TOE environment

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

OT.Prot_Abuse-Func (Protection against Abuse of Functionality) The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard 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

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.

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 [3]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

3.5.2 Security Objectives for the Development and Manufacturing Environment

OD.Assurance (Assurance Security Measures in Development and Manufacturing Environment) The developer and manufacturer ensure that the TOE is designed and fabricated such that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfills its security objectives and is resistant against obvious penetration attacks with high attack potential.

OD.Material (Control over MRTD Material) The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, initialize, pre-personalize genuine MRTD's materials and to personalize authentic MRTDs in order to prevent counterfeit of MRTDs using MRTD materials.

3.5.3 Security Objectives for the Operational Environment

Issuing State or Organization

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

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 Signing 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 Signing 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 [2].

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.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 must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [3]. 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 traveler as MRTD holder. The Inspection Systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all Inspection Systems.

OE.Prot_Logical_MRTD (Protection of data of 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.

OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems) The Document Verifier of receiving States or Organizations authorize 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.

Chapter 4

Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC [14]. Each of these operations is used in this ST.

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

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

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author are denoted as double-underlined text.

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

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

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 $PKPK_{CVCA}$ 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. [4] 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 C_{DV} 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 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 [15] or Elliptic Curve Diffie-Hellman according to ISO 15946 [16].

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
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 Public Key Pair
The Active Authentication Public Key Pair ($SKAA_{ICC}$, $PKAA_{ICC}$) are used for Active Authentication according to TrPKI [3].

Active Authentication Public Key ($PKAA_{ICC}$)
The Active Authentication Public Key ($PKAA_{ICC}$) 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.

Active Authentication Private Key ($SKAA_{ICC}$)
The Active Authentication Private Key ($SKAA_{ICC}$) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.

4.1 Security Functional Requirements for the TOE

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

4.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 [14] extended).

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.
Dependencies:	No dependencies.

4.1.2 Class Cryptographic Support (FCS)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2 [14]). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

Hierarchical to:	No other components.
FCS_CKM.1.1/ KDF_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: TrPKI [3], Annex E.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_CKM.1/DH_MRTD Cryptographic key generation – Diffie-Hellman Keys by the MRTD

Hierarchical to:	No other components.
FCS_CKM.1.1/ DH_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH and specified cryptographic key sizes 112 bits that meet the following: TR-03110 [4], Annex A.1
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2 [14]).

FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to:	No other components.
FCS_CKM.4.1/ MRTD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion of key value that meets the following: FIPS PUB 140-2 [17].
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] FMT_MSA.2 Secure security attributes

Cryptographic Operation (FCS_COP.1)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2 [14]). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to:	No other components.
FCS_COP.1.1/ SHA_MRTD	The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1, SHA-224 and SHA-256 and cryptographic key sizes none that meet the following: FIPS 180-2 [18].
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 FMT_MSA.2 Secure security attributes

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

Hierarchical to:	No other components.
FCS_COP.1.1/ TDES_MRTD	The TSF shall perform Secure Messaging - encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [19] and [3] Annex E.3.
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to:	No other components.
FCS_COP.1.1/ MAC_MRTD	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 [20] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD

Hierarchical to:	No other components.
FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224 or SHA-256 and cryptographic key sizes 224 bit or 256 bit that meet the following: FIPS 186-2 [18].
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/RSA_MRTD Cryptographic operation – Signature creation by MRTD

Hierarchical to:	No other components.
FCS_COP.1.1/ RSA_MRTD	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA with SHA-1 and cryptographic key size 1024 bits that meet the following: ISO/IEC 9796-2:2002 [21].
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 FMT_MSA.2 Secure security attributes

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 [14]).

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to:	No other components.
FCS_RND.1.1/ MRTD	The TSF shall provide a mechanism to generate random numbers that meet the requirements for SOF high defined in AIS20 [22].
Dependencies:	No dependencies.

4.1.3 Class FIA Identification and Authentication

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

Name	**SFR for the TOE**	**SFR for the TOE environment (terminal)**	**Algorithms and key sizes** according to [3], Annex E, and [4]
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/BT, FIA_UAU.6/BT	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/MRTD, FIA_UAU.5/MRTD, FIA_UAU.6/MRTD	FIA_UAU.4/GIS, FIA_UAU.5/GIS, FIA_UAU.6/GIS	ECDH and Retail-MAC, 112 bit keys
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	EC-DSA with SHA
Active Authentication	FIA_API.1/AA	FIA_UAU.4/BT	RSA with 1024 bits. Algorithm according to [3], Annex D

Table 4.1: Overview on authentication SFR

Note the Chip Authentication Protocol include the asymmetric key agreement and 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 TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2 [14]).

FIA_UID.1 Timing of identification

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

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2 [14]).

FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
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 3. to identify themselves by selection of the authentication key on behalf of the user to be performed before the user is identified.
FIA_UAU.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2 [14]).

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

Hierarchical to:	No other components.
FIA_UAU.4.1/ MRTD	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Terminal Authentication Protocol, 3. Authentication Mechanism based on Triple-DES.
Dependencies:	No dependencies.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2 [14]).

FIA_UAU.5/MRTD Multiple authentication mechanisms

Hierarchical to:	No other components.
FIA_UAU.5.1/ MRTD	The TSF shall provide 1. Basic Access Control Authentication Mechanism, 2. Terminal Authentication Protocol, 3. Secure messaging in MAC-ENC mode, 4. Symmetric Authentication Mechanism based on Triple-DES to support user authentication.
FIA_UAU.5.2/ MRTD	The TSF shall authenticate any user's claimed identity according to the following rules: 1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms a. the Basic Access Control Authentication Mechanism with Personalization Agent Keys, b. the Symmetric Authentication Mechanism with Personalization Agent Key, c. the Terminal Authentication Protocol with Personalization Agent Keys. 2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. 3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of Secure Messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism. 4. After run of the Chip Authentication Mechanism 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. 5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses Secure Messaging established by the Chip Authentication Mechanism.
Dependencies:	No dependencies.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2 [14]).

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

Hierarchical to:	No other components.
FIA_UAU.6.1/ MRTD	The TSF shall re-authenticate the user under the conditions 1. Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS. 2. Each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.
Dependencies:	No dependencies.

Authentication failure handling (FIA_AFL.1)

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when 1 unsuccessful authentication attempt occurs related to BAC authentication.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time greater 10 seconds between the reception of the authentication command and its processing.
Dependencies:	FIA_UAU.1 Timing of authentication

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended [14]).

FIA_API.1/CAP Authentication Proof of Identity – MRTD

Hierarchical to:	No other components.
FIA_API.1.1/ CAP	The TSF shall provide a Chip Authentication Protocol according to [4] to prove the identity of the TOE.
Dependencies:	No dependencies.

FIA_API.1/AA Authentication Proof of Identity – MRTD

Hierarchical to:	No other components.
FIA_API.1.1/ AA	The TSF shall provide an Active Authentication Mechanism according to [3] to prove the identity of the TOE.
Dependencies:	No dependencies.

4.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2 [14]).

FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the Access Control SFP on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.
Dependencies:	FDP_ACF.1 Security attribute based access control

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2 [14]).

FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Personalization Agent, b. Basic Inspection System, c. Extended Inspection System d. Terminal, 2. Objects: a. data EF.DG1 to EF.DG16 of the logical MRTD, b. data in EF.COM, c. data in EF.SOD, 3. Security attributes: a. authentication status of terminals, b. Terminal Authorization

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, 3. the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, 4. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization, 5. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules: 1. A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG3, 2. A terminal authenticated as CVCA is not allowed to read to read data in the EF.DG4, 3. A terminal authenticated as DV is not allowed to read to read data in the EF.DG3, 4. A terminal authenticated as DV is not allowed to read to read data in the EF.DG4, 5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2 [14]).

FDP_UCT.1/MRTD Basic data exchange confidentiality – MRTD

Hierarchical to:	No other components.
FDP_UCT.1.1 MRTD	The TSF shall enforce the Access Control SFP to be able to transmit andreceive objects in a manner protected from unauthorized disclosure **after Chip Authentication**.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2 [14]).

FDP_UIT.1/MRTD Data exchange integrity – MRTD

Hierarchical to:	No other components.
FDP_UIT.1.1 MRTD	The TSF shall enforce the Access Control SFP to be able to transmit andreceive user data in a manner protected from modification, deletion, insertion and replay errors **after Chip Authentication**.
FDP_UIT.1.2 MRTD	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred **after Chip Authentication**.
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]

4.1.5 Class FMT Security Management

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2 [14]).

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization 2. Personalization 3. Configuration
Dependencies:	No Dependencies

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2 [14]).

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles 1. Manufacturer 2. Personalization Agent 3. Country Verifier Certification Authority 4. Document Verifier 5. Basic Inspection System 6. Domestic Extended Inspection System 7. Foreign Extended Inspection System
FMT_SMR.1.2	The TSF shall be able to associate users with roles
Dependencies:	FIA_UID.1 Timing of identification

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 [14] extended).

FMT_LIM.1 Limited capabilities

Hierarchical to:	No other components.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. Software to be reconstructed 4. Substantial information about construction of TSF to be gathered which may enable other attacks
Dependencies:	FMT_LIM.2 Limited availability.

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (Common Criteria Part 2 [14] extended).

FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. Software to be reconstructed 4. Substantial information about construction of TSF to be gathered which may enable other attacks
Dependencies:	FMT_LIM.1 Limited capabilities.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2 [14]). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Prepersonalization Data

Hierarchical to:	No other components.
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Prepersonalization Data to the Manufacturer
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ CVCA_INI	The TSF shall restrict the ability to write the 1. Initial Country Verifying Certification Authority Public Key 2. Initial Country Verifier Certification Authority Certificate 3. Initial Current Date to the Personalization Agent
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifying Certification Authority Public Key 2. Country Verifier Certification Authority Certificate to the Country Verifier Certification Authority
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ DATE	The TSF shall restrict the ability to modify the Current date to 1. Country Verifying Certification Authority 2. Document Verifier 3. Domestic Extended Inspection System
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent
Dependencies:	ADV_SPM.1 Informal TOE security policy model FMT_MTD.1 Management of TSF data

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to load the Active Authentication Private Key to the Personalization Agent
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

Hierarchical to:	No other components.
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the 1. Document Basic Access Keys 2. Chip Authentication Private Key 3. Personalization Agent Keys 4. Active Authentication Private Key to none
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
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**
Dependencies:	ADV_SPM.1 Informal TOE security policy model FMT_MTD.1 Management of TSF data

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.

4.1.6 Class FPT Protection of 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 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 SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)” , “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria Part 2 [14] extended).

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
FPT_EMSEC.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to Personalization Agent Authentication Key and Chip Authentication Private Key and Manufacturer Authentication Keysand Active Authentication Private Key.
FPT_EMSEC.1.2	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Authentication Key and Chip Authentication Private Key and Manufacturer Authentication Key and Active Authentication Private Key.
Dependencies:	No dependencies.

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 [14]).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions where therefore a malfunction could occur 2. failure detected by TSF according to FPT_TST.1
Dependencies:	ADV_SPM.1 Informal TOE security policy model

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2 [14]).

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up and at the condition "request of random numbers" to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.
Dependencies:	FPT_AMT.1 Abstract machine testing.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2 [14]).

FPT_PHP.3 Resistance to physical attack

Hierarchical to:	No other components.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.
Dependencies:	No dependencies.

The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

The TOE shall meet the requirement "Non-bypassability of the TSP (FPT_RVM.1)" as specified below (Common Criteria Part 2 [14]).

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to:	No other components.
FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	No dependencies.

The TOE shall meet the requirement "TSF domain separation (FPT_SEP.1)" as specified below (Common Criteria Part 2 [14]).

FPT_SEP.1 TSF domain separation

Hierarchical to:	No other components.
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No dependencies.

4.2 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 taking the following components:

- ADV_IMP.2
- ALC_DVS.2
- AVA_MSU.3
- AVA_VLA.4

The minimum strength of function is SOF-high.

This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

4.3 Security Requirements for the IT Environment

This section describes the security functional requirements for the IT environment using the CC part 2 [14] components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in **bold**.

4.3.1 Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (EF.DG1 to EF.DG16) by means of the Document Security Object. TrPKI [3] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the Issuing State or Organization shall meet the requirement "Basic data authentication (FDP_DAU.1)" as specified below (Common Criteria Part 2 [14]).

FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to:	No other components.
FDP_DAU.1.1/DS	The **Document Signer** shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (EF.DG1 to EF.DG16) and the Document Security Object.
FDP_DAU.1.2/DS	The **Document Signer** shall provide Inspection Systems of Receiving States or Organization with the ability to verify evidence of the validity of the indicated information.
Dependencies:	No dependencies.

4.3.2 Extended Access Control PKI

The CVCA and the DV shall establish a Document Verification PKI by generating asymmetric key pairs and certificates for the CVCA, DV and IS which may be verified by the TOE. The following SFR use the term "PKI" as synonym for entities like CVCA, DV and IS which may be responsible to perform the identified functionality.

FCS_CKM.1/PKI Cryptographic key generation – Document Verification PKI Keys

Hierarchical to:	No other components.
FCS_CKM.1.1/PKI	The **PKI** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDSA and specified cryptographic key sizes 224 bit or 256 bit that meet the following: TR-03110 [4], Annex A .
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_COP.1/CERT_SIGN Cryptographic operation – Certificate Signing

Hierarchical to:	No other components.
FCS_COP.1.1/ CERT_SIGN	The **PKI** shall perform digital signature creation in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 224 bit or 256 bit that meet the following: TR-03110 [4].
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 FMT_MSA.2 Secure security attributes

4.3.3 Basic Terminal

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called "Basic Terminals" (BT) in this section.

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2 [14]).

FCS_CKM.1/KDF_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal

Hierarchical to:	No other components.
FCS_CKM.1.1/ KDF_BT	The **Basic Terminal** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: TrPKI [3].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FDP_ITC.2 Import of user data with security attributes, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2 [14]).

FCS_CKM.4/BT Cryptographic key destruction – BT

Hierarchical to:	No other components.
FCS_CKM.4.1/BT	The **Basic Terminal** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with zeros or random data that meets the following: FIPS PUB 140-2 [17].
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] FMT_MSA.2 Secure security attributes

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2 [14]). The iterations are caused by different cryptographic algorithms to be implemented by the Basic Terminal.

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

Hierarchical to:	No other components.
FCS_COP.1.1/ SHA_BT	The **Basic Terminal** shall perform hashing in accordance with a specified cryptographic algorithms SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2 [18].
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to:	No other components.
FCS_COP.1.1/ ENC_BT	The **Basic Terminal** shall perform Secure Messaging - encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [19], ISO 11568-2 [23], ISO 9797-1 [24] (padding mode 2).
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

Hierarchical to:	No other components.
FCS_COP.1.1/ MAC_BT	The **Basic Terminal** shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm Retail-MAC and cryptographic key sizes 112 bit that meet the following: FIPS 46-3 [19], ISO 9797 [20] (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2).
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/RSA_BT Cryptographic operation – RSA

Hierarchical to:	No other components.
FCS_COP.1.1/ RSA_BT	The **Basic Terminal** shall perform digital signature verification in accordance with a specified cryptographic algorithm RSA with SHA-1 and cryptographic key sizes 1024 bit that meet the following: Scheme 1 of ISO/IEC 9796-2: [21].
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 FMT_MSA.2 Secure security attributes

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Quality metric for random numbers (FCS_RND.1" as specified below (Common Criteria Part 2 [14]).

FCS_RND.1/BT Quality metric for random numbers – Basic Terminal

Hierarchical to:	No other components.
FCS_RND.1.1/BT	The **Basic Terminal** shall provide a mechanism to generate random numbers that meets the requirements for SOF high defined in AIS20 [22].
Dependencies:	No dependencies.

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2 [14]).

FIA_UAU.4/BT Single-use authentication mechanisms – Basic Terminal

Hierarchical to:	No other components.
FIA_UAU.4.1/BT	The **Basic Terminal** shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism and Active Authentication Mechanism.
Dependencies:	No dependencies.

The Basic Terminal of the Issuing State or Organization shall meet the requirement "Re-authentication (FIA_UAU.6)" as specified below (Common Criteria Part 2 [14]).

FIA_UAU.6/BT Re-authentication – Basic Terminal

Hierarchical to:	No other components.
FIA_UAU.6.1/BT	The **Basic Terminal** shall shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism.
Dependencies:	No dependencies.

4.3.4 General Inspection System

The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. Therefore it has to fulfill all security requirements of the Basic Inspection System as described above.

The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new Secure Messaging with keys. The reference data for the Chip Authentication Mechanism is the Chip Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

The General Inspection System of the Issuing State or Organization shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2 [14])

FCS_CKM.1/DH_GIS Cryptographic key generation – Diffie-Hellman Keys by the GIS

Hierarchical to:	No other components.
FCS_CKM.1.1/ DH_GIS	The **General Inspection System** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH, Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [4] Annex A.1.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_COP.1/SHA_GIS Cryptographic operation – Hash for Key Derivation by GIS

Hierarchical to:	No other components.
FCS_COP.1.1/ SHA_GIS	The **General Inspection System** shall perform hashing in accordance with a specified cryptographic algorithm SHA-1, SHA-224 and SHA-256 and cryptographic key sizes none that meet the following: FIPS 180-2 [18].
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 FMT_MSA.2 Secure security attributes

The General Inspection System of the Issuing State or Organization shall meet the requirement "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2 [14])

FIA_UAU.4/GIS Single-use authentication mechanisms – Single-use authentication of the Terminal by the GIS

Hierarchical to:	No other components.
FIA_UAU.4.1/GIS	The **General Inspection System** shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism 2. Chip Authentication Protocol
Dependencies:	No dependencies.

The General Inspection System of the Issuing State or Organization shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2 [14])

FIA_UAU.5/GIS Multiple authentication mechanisms – General Inspection System

Hierarchical to:	No other components.
FIA_UAU.5.1/GIS	The **General Inspection System** shall provide 1. Basic Access Control Authentication Mechanism 2. Chip Authentication Protocol to support user authentication.
FIA_UAU.5.2/GIS	The **General Inspection System** shall authenticate any user's claimed identity according to the following rules: 1. The General Inspection System accepts the authentication attempt as MRTD only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. 2. After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of Secure Messaging with key agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism. 3. After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of Secure Messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
Dependencies:	No dependencies.

The General Inspection System of the Issuing State or Organization shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2 [14])

FIA_UAU.6/GIS Re-authenticating – Re-authenticating of Terminal by the General Inspection System

Hierarchical to:	No other components.
FIA_UAU.6.1/GIS	The **General Inspection System** shall re-authenticate the user under the conditions 1. Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of Secure Messaging keys agreed upon by the Basic Access Control Authentication Mechanism. 2. Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of Secure Messaging keys generated by Chip Authentication Protocol.
Dependencies:	No dependencies.

The General Inspection System of the Issuing State or Organization shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2 [14])

FD_UCT.1/GIS Basic data exchange confidentiality – General Inspection System

Hierarchical to:	No other components.
FDP_UCT.1.1/GIS	The **General Inspection System** shall enforce the Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure **after Chip Authentication**.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

The General Inspection System of the Issuing State or Organization shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2 [14])

FDP_UIT.1/GIS Data exchange integrity – General Inspection System

Hierarchical to:	No other components.
FDP_UIT.1.1/GIS	The **General Inspection System** shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors **after Chip Authentication**.
FDP_UIT.1.2/GIS	The **General Inspection System** shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred **after Chip Authentication**.
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]

4.3.5 Extended Inspection System

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.

FCS_COP.1/SIG_SIGN_EIS Cryptographic operation – Signature creation by EIS

Hierarchical to:	No other components.
FCS_COP.1.1/ SIG_SIGN_EIS	The **Extended Inspection System** shall perform signature creation in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 224 bit or 256 bit that meet the following: ISO 15946-2 [25].
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 FMT_MSA.2 Secure security attributes

FCS_COP.1/SHA_EIS Cryptographic operation – Hash for Key Derivation by EIS

Hierarchical to:	No other components.
FCS_COP.1.1/ SHA_EIS	The **Extended Inspection System** shall perform hashing in accordance with a specified cryptographic algorithm SHA-1, SHA-224 and SHA-256 and cryptographic key sizes none that meet the following: FIPS 180-2 [18].
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 FMT_MSA.2 Secure security attributes

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 [14] extended)

FCS_COP.1/SHA_EIS Cryptographic operation – Hash for Key Derivation by EIS

Hierarchical to:	No other components.
FIA_API.1.1/EIS	The **Extended Inspection System** shall provide a Terminal Authentication Protocol according to TR-03110 [4] to prove the identity of the Extended Inspection system.
Dependencies:	No dependencies.

4.3.6 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

1. The Basic Access Control Mechanism which may be used by the Personalization Terminal with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the Secure Messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

2. The Personalization Terminal may use the Terminal Authentication Protocol like a Extended Inspection System but using the Personalization Agent Keys to authenticate themselves to the TOE. This approach may be used in a personalization environment where (i) the Personalization Agent want to authenticate the MRTD's chip and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.

3. In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without Secure Messaging. Therefore the TOE and the Personalization Terminal support a simple the Symmetric Authentication Mechanism with Personalization Agent Key as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

The Personalization Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 [14] extended) if it uses the Symmetric Authentication Mechanism with Personalization Agent Key.

FIA_API.1/SYM_PT Authentication Proof of Identity – Personalization Terminal Authentication with Symmetric Key

Hierarchical to:	No other components.
FIA_API.1.1/SYM_PT	The **Personalization Terminal** shall provide an Authentication Mechanism based on Triple-DES to prove the identity of the Personalization Agent.
Dependencies:	No dependencies.

Chapter 5

TOE Summary Specification

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

5.1 TOE Security Functions

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

In the following table all TOE Security Functions with an SOF claim are listed. The assessment of cryptographic algorithms is not part of this CC evaluation.

TOE Security Function	SOF claim	Description
F.IC_CL	high	The functionality is defined in BSI-DSZ-CC-0417
F.Identification_Authentication	high	The mechanism for identification/ authentication of the roles is probabilistic
F.Crypto	high	The mechanism for identification/ authentication and confidentiality of communication is probabilistic.

Table 5.1: TOE Security Functions with SOF Claim

5.1.1 TOE Security Functions from Hardware (IC) and Crypto Library

F.IC_CL: Security Functions of the Hardware (IC) and Crypto Library

This Security Function covers the security functions of the hardware (IC) as well as of the crypto library and is composed in particular of

- Generation of random number used in the anticollision phase of the chip in phase 4 to create communication identification data and the creation of a session key and authen-

tication nonces; the seed is created by the hardware-realized random number generator (RNG) and is used by the software-realized RNG

- Triple-DES co-processor to support DES calculations is used in all cases where DES/3DES is used
- Internal security measures which clear memory areas used by the Crypto Library after usage
- Copy memory content in a manner protected against side channel attacks
- Control of operating conditions
- Protection against physical manipulations
- Logical protection includes software countermeasures against side channel attacks
- Protection of mode control especially used to store the chip identification data in the User Read Only Area and to separate security domains
- ECC Signature Generation and Verification
- ECC Diffie-Hellman Key Exchange
- RSA algorithm

The supported SHA and AES algorithms as well as ECC and RSA key generation are not used.

5.1.2 TOE Security Functions from Embedded Software (ES) – Operating system

F.Access_Control

This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. This function consists of following elements:

1. Access to objects is controlled based on subjects, objects (any file) and security attributes
2. No access control policy allows reading of any key
3. Any access not explicitly allowed is denied
4. Access Control in phase 2 – initialization and pre-personalization – enforces initialization policy: Configuration and initialization of the TOE only by the manufacturer or on behalf of him (see F.Management) respectively pre-personalization policy: Configuring of Access Control policy, doing key management and reading of initialization data only by the Manufacturer (prepersonalization agent) identified with its authentication key (see F.Management)

5. Access Control in phase 3 – personalization – enforces personalization policy: Writing of user data, keys (Basic Access Control, Active Authentication, Chip Authentication) and Terminal Authentication data (CVCA data and current date) and reading of initialization data only by the personalization agent identified with its authentication key (see F.Management)

6. Access Control in phase 4 – operation – enforces operational use policy as described in TR-03110 [4]: Reading of optional biometrics (EF.DG3, EF.DG4) by authenticated and authorized EIS; Active Authentication, Chip Authentication, Terminal Authentication and reading of other user data by BIS, GIS and EIS authenticated at least by Secure Messaging with BAC.

F.Identification_Authentication

This function provides identification/authentication of the user roles

- Manufacturer (Initialization/Pre-personalization Agent)
- Personalization Agent
- Country Verifier Certification Authority
- Document Viewer
- Basic Inspection System
- Extended Inspection System (domestic/foreign)

by the methods:

- Symmetric BAC authentication method [3] with following properties
  - The authentication is as specified by ICAO
  - It uses a challenge from the MRTD
  - The method can be configured by the administrator to delay the processing of the authentication command after a failed authentication command of up to over 10 seconds
  - The cryptographic method for confidentiality is Triple-DES/CBC provided by F.Crypto
  - The cryptographic method for authenticity is DES/Retail MAC provided by F.Crypto
  - On error (wrong MAC, wrong challenge) the user role is not identified/authenticated
  - On success the session keys are created and stored for Secure Messaging
- Secure Messaging with following properties
  - The Secure Messaging is as specified by ICAO
  - The cryptographic method for confidentiality is Triple-DES/CBC provided by F.Crypto

  - The cryptographic method for authenticity is DES/Retail MAC provided by F.Crypto
  - In a Secure Messaging protected command the method for confidentiality and the method for authenticity must be present
  - The initialization vector is an encrypted send sequence counter (SSC)
  - In phases 3 - 4 a session key is used
  - On any non correctly with the session keys protected command the session keys are overwritten according to FIPS 140-2 [17] (or better) and a new BAC authentication is required
  - Overwrites keys in transient memory after usage
- Active Authentication with following properties
  - According to TrPKI [3] using RSA from F.IC_CL
- Chip Authentication with following properties
  - According to TR-03110 [4] using ECDH from F.IC_CL
  - Session keys are created and stored for Secure Messaging replacing existing session keys.
- Terminal Authentication with following properties
  - According to TR03110 [4] checking certificates with ECDSA from F.IC_CL
  - It uses a challenge from the MRTD
  - Usable only in a Secure Messaging session with Chip Authentication key
  - It distinguishes between the roles
    * Country Verifier Certification Authority
    * Domestic and foreign Document Verifier
    * Domestic and foreign Extended Inspection System
  - Update of CVCA certificate is allowed for CVCA
  - Update of current date is allowed for CVCA, domestic and foreign Document Verifier and domestic Extended Inspection System
  - Only with a public key from an IS certificate the challenge-response authentication itself is performed
  - The bitwise AND of the Certificate Holder Authorizations of a certificate chain is used for Terminal Authorization
  - Verifying validity of certificate chain
    * Certificates must be in the sequence: known CVCA [> CVCA]> DV > IS
    * Expiration dates must not be before the current date

F.Management

In phase 2 the Manufacturer (Initialization/Pre-personalization Agent) performs the initialization and configures the file layout including security attributes by sending an install script to the TOE. The script is prepared by the developer and protected with Secure Messaging. In this process the TOE is configured for the ICAO application (e.g. random UID). The layout determines that the parameters given in F.Access_Control for phases 3 and 4 are enforced. The agent can also do key management and other administrative tasks.

In phase 3 the Personalization Agent performs following steps:

- Formatting of all data to be stored in the TOE according to ICAO requirements which are outside the scope of the TOE. The data to be formatted includes the index file, data groups, Passive Authentication data, BAC key derived from the Machine Readable Zone data, Active Authentication Private Key, Chip Authentication Private Key and Terminal Authentication CVCA Public Keys and parameters
- Writing of all the required data to the appropriate files as specified in TrLDS [2]
- Changing the TOE into the end-usage mode for phase 4 where reading of the initialization data is prevented

F.Crypto

This function provides a high level interface to

- DES (supplied by F.IC_CL)
- Triple-DES/CBC
- DES/Retail MAC

This function implements the hash algorithms according to FIPS 180-2 [18]

- SHA-1
- SHA-224
- SHA-256

F.Verification

TOE internal functions ensures correct operation.

5.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 are

Assurance Measure	**Description**
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation and startup
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_LLD.1	Implementation of the TSF
ADV_IMP.2	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: High-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.3	Analysis and testing for insecure states
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.4	Highly resistant

Table 5.2: Assurance Measures

Chapter 6

PP Claims

6.1 PP Reference

The conformance of this ST to the Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.2, BSI-PP-0026 is claimed.

6.2 PP Refinements

None

6.3 PP Additions

Active Authentication based on ICAO PKI v1.1 [3] has been added. The added and modified SFRs are listed in section 7.3.

Chapter 7

Rationale

7.1 Security Objectives Rationale

The following table provides an overview for security objectives coverage. In comparison with BSI-PP-0026 the table includes the following corrections: T.Chip-ID is countered by OT.Data_Conf, not OT.Sens_Data_Conf; Active Authentication is supported.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	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	OD.Assurance	OD.Material	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System	OE.Active_Auth_Key_MRTD
T.Chip-ID			x		x															x		
T.Skimming			x																			
T.Read_Sensitive_Data				x													x				x	
T.Forgery	x	x							x						x			x	x			
T.Counterfeit						x					x		x			x		x				x
T.Abuse-Func							x															
T.Information_Leakage								x														
T.Phys-tamper									x													
T.Malfunction										x												
P.Manufact												x	x									
P.Personalization	x											x		x								
P.Personal_Data		x	x																	x		
P.Sensitive_Data				x													x			x		
A.Pers_Agent														x								
A.Insp_Sys																		x		x		
A.Signature_PKI															x			x				
A.Auth_PKI																	x				x	

Table 7.1: Security Objective Rationale

The OSP **P.Manufact** "Manufacturing of the MRTD's chip" requires the quality and integrity of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing including unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data. The security objective for the TOE environment **OD.Assurance** "Assurance Security Measures in Development and Manufacturing Environment" address these obligations of the IC Manufacturer and MRTD Manufacturer. **OD.Material** "Control over MRTD material" ensures that materials, equipment and tools used to produce genuine and authentic MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs.

The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the enrollment 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 Authentication key(s) according to **OD.Assurance** "Assurance Security Measures in Development and Manufactur-

ing Environment". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

The OSP **P.Personal_Data** "Personal data protection policy" requires that the logical MRTD can be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an Inspection System. This OSP is covered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the Secure Messaging based on session keys agreed in this protocol. The security objective **OT.Data_Conf** requires the TOE to implement the Basic Access Control as defined by ICAO [2] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the Inspection System to protect their communication with the TOE before Secure Messaging is successfully established based on the Chip Authentication Protocol. After successful Chip Authentication the security objective **OT.Data_Conf** "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

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.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered by security objectives for the TOE and the TOE environment depending on the use of the Chip Authentication Protocol and the Secure Messaging based on session keys agreed in this protocol. The security objective **OT.Identification** "Identification and Authentication of the TOE" by limiting the TOE chip identification to the Basic Inspection System. The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" requires the Inspection System to protect to their communication (as Basic Inspection System) with the TOE before Secure Messaging based on the Chip Authentication Protocol is successfully established. After successful Chip Authentication the security objective **OT.Data_Conf** "Confidentiality of personal data" ensures the confidentiality of the logical MRTD data during their transmission to the General Inspection System.

The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" addresses the reading of the logical MRTD trough the contactless interface outside the communication between the MRTD's chip and Inspection System. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through Basic Access Control allowing read data access only after successful authentication of the Basic Inspection System.

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 a 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. MRTDs must be controlled in order to prevent their usage for production of counterfeit MRTDs targeted on by **OD.Material**. 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 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.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 enrollment, the protection with digital signature and the storage of the MRTD holder personal data and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the Basic Access Control.

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 of 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 biometric 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.

7.2 Security Requirements Rationale

7.2.1 Security Functional Requirements Rationale

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

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.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/KDF_MRTD	x	x	x	x		x					
FCS_CKM.1/DH_MRTD	x	x		x		x					
FCS_CKM.4/MRTD	x	x	x	x							
FCS_COP.1/SHA_MRTD	x	x	x	x		x					
FCS_COP.1/TDES_MRTD	x	x	x			x					
FCS_COP.1/MAC_MRTD	x	x	x	x		x					
FCS_COP.1/SIG_VER	x			x							
FCS_COP.1/RSA_MRTD											x
FCS_RND.1/MRTD	x			x							
FIA_UID.1	x	x	x	x	x						
FIA_UAU.1	x	x	x	x	x						
FIA_UAU.4/MRTD	x	x	x	x							
FIA_UAU.5/MRTD	x	x	x	x							
FIA_UAU.6/MRTD	x	x	x	x							
FIA_AFL.1			x								
FIA_API.1/CAP						x					
FIA_API.1/AA											x
FDP_ACC.1	x	x	x	x							
FDP_ACF.1	x	x	x	x							
FDP_UCT.1/MRTD			x	x							
FDP_UIT.1/MRTD		x		x							
FMT_SMF.1	x	x	x								
FMT_SMR.1	x	x	x								
FMT_LIM.1							x				
FMT_LIM.2							x				
FMT_MTD.1/INI_ENA					x						
FMT_MTD.1/INI_DIS					x						
FMT_MTD.1/CVCA_INI				x							
FMT_MTD.1/CVCA_UPD				x							
FMT_MTD.1/DATE				x							
FMT_MTD.1/KEY_WRITE	x		x								
FMT_MTD.1/CAPK		x	x	x		x					
FMT_MTD.1/AAPK											x
FMT_MTD.1/KEY_READ	x	x	x	x		x					x
FMT_MTD.3				x							
FPT_EMSEC.1	x							x			
FPT_TST.1								x		x	
FPT_RVM.1							x				
FPT_FLS.1								x		x	
FPT_PHP.3								x	x		
FPT_SEP.1							x			x	

Table 7.2: 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 and the management of the TSF for Basic Access Control. 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/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/MRTD and FIA_UAU.5/MRTD. If the Basic Access Control Authentication Mechanism with the Personalization Agent Authentication Key is used the TOE will use the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1/MRTD (for the generation of the challenge), FCS_CKM.1/DH_MRTD, FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/MRTD (for the re-authentication). If the Personalization Terminal wants to authenticate themselves 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/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.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 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/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The SFR FIA_UAU.6/MRTD and FDP_UIT.1/MRTD requires the integrity protection of the transmitted data after chip authentication by means of Secure Mes-

saging implemented by the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use.

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

The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data in EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: only the successful authenticated Personalization Agent, Basic Inspection Systems[1] and Extended Inspection Systems are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

The SFR FIA_AFL.1 strengthens the authentication function as terminal part of the Basic Access Control Authentication Protocol or other authentication functions if necessary. The SFR FIA_UAU.4/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5/MRTD enforces the TOE (i) to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and (ii) to accept chip authentication only after successful authentication as Basic Inspection System. Moreover, the SFR FIA_UAU.6/MRTD requests Secure Messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism.

After Chip authentication the TOE and the General Inspection System establish protection of the communication by Secure Messaging (cf. the SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) in ENC_MAC_Mode by means of the cryptographic functions according to FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The security objective **OT.Sense_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.

[1] Note that the General Inspection Systems use the role Basic Inspection System.

The SFR FIA_UID.1 and FIA_UAU.1 requires authentication of the Inspection Systems. The SFR FIA_UAU.5/MRTD requires the successful Chip Authentication before any authentication attempt as Extended Inspection System. The SFR FIA_UAU.6/MRTD and FDP_UCT.1/MRTD 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/MRTD (for the generation of the terminal authentication challenge), FCS_CKM.1/DH_MRTD (for the generation of shared secret), FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the new session keys), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode Secure Messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.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 TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their use in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt.

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/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/DH_MRTD is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [4] requires additional TSF according to FCS_CKM.1/KDF_MRTD, FCS_COP.1/SHA_MRTD (for the derivation of the session keys), FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging).

The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by (i) the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other which may not be used after TOE Delivery, (ii) the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and (iii) the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

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, (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction, and (iii) the SFR FPT_SEP.1 limiting the effects of malfunctions due to TSF domain separation.

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/KEY_READ. The Active Authentication Protocol [3] requires additional TSF according to FCS_COP.1/RSA_MRTD.

The security objectives **OD.Assurance** and **OD.Material** for the IT environment will be supported by non-IT security measures only.

The security objective **OE.Authoriz_Sens_Data** is directed to establish the Document Verifier PKI and will be supported by non-IT security measures only.

The following table provides an overview how security functional requirements for the IT environment cover security objectives for the TOE environment. The security target describes only those SFR of the IT environment directly related to the SFR for the TOE.

	OE.Personalization	OE.Pass_Auth_Sign	OE.Auth_Key_MRTD	OE.Authoriz_Sens_Data	OE.Exam_MRTD	OE.Pass_Auth_Verif	OE.Prot_Logical_MRTD	OE.Ext_Insp_System	OE.Active_Auth_Key_MRTD
Document Signer									
FDP_DAU.1/DS		x	x		x	x			x
Document Verification PKI									
FCS_CKM.1/PKI				x					
FCS_COP.1/CERT_SIGN				x					
Basic Inspection System									
FCS_CKM.1/KDF_BT	x				x		x		
FCS_CKM.4/BT					x		x		
FCS_COP.1/SHA_BT	x				x		x		
FCS_COP.1/ENC_BT	x				x		x		
FCS_COP.1/MAC_BT	x				x		x		
FCS_COP.1/RSA_BT									x
FCS_RND.1/BT	x				x		x		
FIA_UAU.4/BT	x				x		x		x
FIA_UAU.6/BT	x				x		x		
General Inspection System									
FCS_CKM.1/DH_GIS	x				x				
FCS_COP.1/SHA_GIS	x				x				
FIA_UAU.4/GIS					x				
FIA_UAU.5/GIS					x	x	x	x	
FIA_UAU.6/GIS					x	x	x	x	
FDP_UCT.1/GIS	x				x	x	x	x	
FDP_UIT.1/GIS	x				x	x	x	x	
Extended Inspection System									
FCS_COP.1/SIG_SIGN_EIS	x							x	
FCS_COP.1/SHA_EIS	x							x	
FIA_API.1/EIS	x							x	
Personalization Agent									
FIA_API.1/SYM_PT	x								

Table 7.3: Coverage of Security Objectives for the IT environment by SFR

The **OE.Personalization** "Personalization of logical MRTD requires the Personalization Terminal to authenticate themselves to the MRTD's chip to get the write authorization.

If the Basic Access Control Authentication Mechanism with the Personalization Agent Au-

thentication Key is used the Personalization Terminal will use the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT (for the derivation of the session keys), and FCS_COP.1/ENC_BT and FCS_COP.1/MAC_BT (for the ENC_MAC_Mode Secure Messaging) and to authenticate themselves and to protect the personalization data during transfer.

If the Personalization Terminal want to authenticate themselves to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the Personalization Terminal will use TSF according to the FCS_RND.1/BT (for the generation of the challenge), FCS_CKM.1/DH_GIS, FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_GIS (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/ TDES_MRTD and FCS_COP.1/MAC_MRTD (for the ENC_MAC_Mode Secure Messaging), FCS_COP.1/SIG_SIGN_EIS, FCS_COP.1/SHA_EIS and FIA_API.1/EIS (as part of the Terminal Authentication Protocol).

If the Personalization Terminal wants to authenticate themselves to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the SFR FIA_API.1/SYM_PT, FCS_RND.1/MRTD (for the generation of the challenge) and FCS_COP.1/TDES_MRTD (to verify the authentication attempt). Using the keys derived by means of the Chip Authentication Mechanism the Personalization Agent will transfer MRTD holder's personalization data (identity, biographic data, correctly enrolled biometric reference data) in a confidential and integrity protected manner as required by FDP_UCT.1/GIS and FDP_UIT.1/GIS.

The **OE.Pass_Auth_Sign** "Authentication of logical MRTD Signature" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of EF.DG1 to EF.DG16 and the Document Security Objects and therefore, to support the Inspection System to verify the logical MRTD.

The **OE.Auth_Key_MRTD** "MRTD Authentication Key" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of chip authentication public key in DG 14. There is no need for the ST to provide any specific requirement for the method of generation, distribution and handling of the Chip Authentication Private Key by the IT environment.

The **OE.Authoriz_Sens_Data** "Authorization for Use of Sensitive Biometric Reference Data"
addresses the establishment of the Document Verification PKI which include cryptographic key generation for the Document Verification PKI Keys and the signing of the certificates. The SFR FCS_CKM.1/PKI and FCS_COP.1/CERT_SIGN enforce that these cryptographic functions fit the signature verification function for the certificates and the terminal authentication addressed by FCS_COP.1/SIG_VER.

The **OE.Exam_MRTD** "Examination of the MRTD passport book" requires the Basic Inspection System for global interoperability to implement the terminal part of the Basic Access Control [2] as required by FCS_CKM.1/KDF_BT, FCS_CKM.4/BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT, FCS_RND.1/BT, FIA_UAU.4/BT and FIA_UAU.6/BT. The verification of the authenticity of the MRTD's chip by General Inspection Systems and Extended Inspection Systems (including the functionality of the GIS) is covered by the FCS_CKM.1/DH_GIS, FCS_COP.1/SHA_GIS, FIA_UAU.4/GIS, FIA_UAU.5/GIS and FIA_UAU.6/GIS providing the Chip Authentication Protocol and checking continuously the

messages received from the MRTD's chip. The authenticity of the Chip Authentication Public Key (EF.DG14) is ensured by FDP_DAU.1/DS.

The **OE.Pass_Auth_Verif** "Verification by Passive Authentication" is covered by the SFR FDP_DAU.1/DS.

The security objective **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" addresses the protection of the logical MRTD during the transmission and internal handling. The SFR FIA_UAU.4/BT, FIA_UAU.5/GIS and FIA_UAU.6/BT address the terminal part of the Basic Access Control Authentication Mechanism and FDP_UCT.1/GIS and FDP_UIT.1/BT the Secure Messaging established by the Chip Authentication mechanism. The SFR FCS_CKM.1/KDF_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT as well as FCS_CKM.4/BT are necessary to implement this mechanism. The BIS shall destroy the Document Access Control Key and the Secure Messaging keys after inspection of the MRTD according to FCS_CKM.4 because they are not needed any more.

The **OE.Ext_Insp_System** "Authorization of Extended Inspection Systems" is covered by the Terminal Authentication Protocol proving the identity of the EIS as required by FIA_API.1/EIS basing on signature creation as required by FCS_COP.1/SIG_SIGN_EIS and including a hash calculation according FCS_COP.1/SHA_EIS.

The **OE.Active_Auth_Key_MRTD** "MRTD Authentication Key" is covered by FDP_DAU.1/DS which requires the Document Signer to provide a capability to generate evidence for the validity of Active Authentication public key in DG15. FCS_COP.1/RSA_BT is necessary to implement this mechanism. FIA_UAU.4/BT address the terminal part of the Active Authentication Mechanism. There is no need for the PP to provide any specific requirement for the method of generation, distribution and handling of the Active Authentication Private Key by the IT environment.

For dependency rationale (SFR/SAR) see BSI-PP-0026 7.2.2 [26]. The following table shows the dependencies of the additional and extended SFRs (see also 7.3).

SFR	Dependencies	Support of the Dependencies
Of the TOE		
FCS_COP.1/RSA_MRTD	[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, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, see below for the justification for non-satisfied dependencies
FIA_API.1/AA	No dependencies	n.a.
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled
FPT_EMSEC.1	No dependencies	n.a.
Of the IT Environment		
FCS_COP.1.1/RSA_BT	[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, FMT_MSA.2 Secure security attributes	FCS_CKM.1, FCS_CKM.4, see below for the justification for non-satisfied dependencies
FIA_UAU.4/BT	No dependencies	n.a.

Table 7.4: Dependencies between the SFRs of the TOE and of the IT Environment

Justification for non-satisfied dependencies between the SFR: The SFRs FCS_COP.1/ RSA_MRTD and FCS_COP.1.1/RSA_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated BIS or MRTD, respectively, only. There is no need for any special security attributes for the secure messaging keys.

7.2.2 TOE Summary Specification Rationale

This shows the coverage of the SFRs by TSFs.

SFR	TSFs
FAU_SAS.1	F.IC_CL
FCS_CKM.1/KDF_MRTD	F.Identification_Authentication
FCS_CKM.1/DH_MRTD	F.IC_CL
FCS_CKM.4/MRTD	F.Identification_Authentication
FCS_COP.1/SHA_MRTD	F.Crypto
FCS_COP.1/TDES_MRTD	F.IC_CL, F.Crypto
FCS_COP.1/MAC_MRTD	F.IC_CL, F.Crypto
FCS_COP.1/SIG_VER	F.IC_CL
FCS_COP.1/RSA_MRTD	F.IC_CL
FCS_RND.1/MRTD	F.IC_CL
FIA_UID.1	F.Access_Control
FIA_UAU.1	F.Access_Control
FIA_UAU.4/MRTD	F.Identification_Authentication
FIA_UAU.5/MRTD	F.Access_Control, F.Identification_Authentication
FIA_UAU.6/MRTD	F.Identification_Authentication
FIA_AFL.1	F.Identification_Authentication
FIA_API.1/CAP	F.Identification_Authentication
FIA_API.1/AA	F.Identification_Authentication
FDP_ACC.1	F.Access_Control
FDP_ACF.1	F.Access_Control
FDP_UCT.1/MRTD	F.Identification_Authentication
FDP_UIT.1/MRTD	F.Identification_Authentication
FMT_SMF.1	F.Management
FMT_SMR.1	F.Identification_Authentication
FMT_LIM.1	F.IC_CL
FMT_LIM.2	F.IC_CL
FMT_MTD.1/INI_ENA	F.IC_CL, F.Access_Control
FMT_MTD.1/INI_DIS	F.Access_Control, F.Management
FMT_MTD.1/CVCA_INI	F.Access_Control
FMT_MTD.1/CVCA_UPD	F.Identification_Authentication
FMT_MTD.1/DATE	F.Identification_Authentication
FMT_MTD.1/KEY_WRITE	F.Access_Control
FMT_MTD.1/CAPK	F.Access_Control
FMT_MTD.1/AAPK	F.Access_Control
FMT_MTD.1/KEY_READ	F.Access_Control
FMT_MTD.3	F.Identification_Authentication
FPT_EMSEC.1	F.IC_CL
FPT_FLS.1	F.IC_CL
FPT_TST.1	F.IC_CL, F.Verification
FPT_PHP.3	F.IC_CL
FPT_RVM.1	F.Access_Control
FPT_SEP.1	F.IC_CL

Table 7.5: Coverage of SFRs for the TOE by TSFs.

The SFR **FAU_SAS.1** requires the storage of the chip identification data which is addressed in **F.IC_CL**.

The SFR **FCS_CKM.1/KDF_MRTD** requires the BAC key derivation algorithm, which is supplied by the BAC authentication mechanism of **F.Identification_Authentication**.

The SFR **FCS_CKM.1/DH_MRTD** requires the ECDH algorithm. This is provided by the crypto library function **F.IC_CL**.

The SFR **FCS_CKM.4/MRTD** requires the destroying of cryptographic keys. This is done in **F.Identification_Authentication** ("Overwrites keys in transient memory after usage").

The SFR **FCS_COP.1/SHA_MRTD** requires SHA-1, SHA-224 and SHA-256. **F.Crypto** provides these hash algorithms.

The SFR **FCS_COP.1/TDES_MRTD** requires Triple-DES in CBC mode and cryptographic key size 112 bit to perform Secure Messaging - encryption and decryption. This is provided in **F.IC_CL** (Triple-DES Co-processor) and **F.Crypto** (provides Triple-DES/CBC and DES/Retail MAC).

The SFR **FCS_COP.1/MAC_MRTD** requires Triple-DES in Retail MAC mode and cryptographic key size 112 bit to perform Secure Messaging - message authentication code. This is provided in **F.IC_CL** (Triple-DES Co-processor) and **F.Crypto** (provides Triple-DES/CBC and DES/Retail MAC).

The SFR **FCS_COP.1/SIG_VER** requires ECDSA and a cryptographic key size of 224 bit or 256 bit to perform digital signature verification. **F.IC_CL** provides functions to verify signatures based on ECC.

The SFR **FCS_COP.1/RSA_MRTD** requires an RSA signature creation according to scheme 1 of ISO/IEC 9796-2 [21] which is provided by **F.IC_CL**.

The SFR **FCS_RND.1/MRTD** requires the generation of random numbers which is provided by **F.IC_CL**. The provided random number generator produces cryptographically strong random numbers which are used at the appropriate places as written in the addition there.

The SFR **FIA_UID.1** requires timing of identification. It is handled by **F.Access_Control** which enforces identification of a role before access is granted ("...only executed after this TSF allowed access"). Also all policies prevent reading sensitive or user dependent data without user identification.

The SFR **FIA_UAU.1** requires timing of authentication. It is handled by **F.Access_Control** which enforces authentication of a role before access is granted ("...only executed after this TSF allowed access"). Also all policies prevent reading sensitive or user dependent data without user authentication.

The SFR **FIA_UAU.4/MRTD** requires prevention of authentication data reuse. This is in particular fulfilled by using changing initialization vectors in Secure Messaging. Secure Messaging is provided by **F.Identification_Authentication**.

The SFR **FIA_UAU.5/MRTD** requires Basic Access Control authentication mechanism, terminal authentication protocol, Secure Messaging in MAC-ENC mode and symmetric authentication mechanism based on Triple-DES. In addition SFR **FIA_UAU.5/MRTD** also requires the authentication of any user's claimed identity. **F.Identification_Authentication** and **F.Access_Control** fulfill these requirements.

The SFR **FIA_UAU.6/MRTD** requires re-authentication for each command after successful authentication. This is done by **F.Identification_Authentication** providing Secure Messaging.

The SFR **FIA_AFL.1** requires the detection of an unsuccessful authentication attempt and the waiting for a specified time between the reception of an authentication command and its processing. **F.Identification_Authentication** detects unsuccessful authentication attempts and can be used "to delay the processing of the authentication command after a failed authentication command".

The SFR **FIA_API.1/CAP** requires the proving of the identity of the TOE. The Chip Authentication is done by **F.Identification_Authentication**.

The SFR **FIA_API.1/AA** requires the proving of the identity of the TOE. The Active Authentication is done by **F.Identification_Authentication**.

The SFR **FDP_ACC.1** requires the enforcement of the access control policy on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16. This is done by F.Access_Control (based on the objects: "a. data EF.DG1 to EF.DG16 ...").

The SFR **FDP_ACF.1** requires the enforcement of the access control policy which is done by **F.Access_Control** ("Access to objects is controlled based on subjects, objects (any files) and security attributes").

The SFR **FDP_UCT.1/MRTD** requires the transmitting and receiving data protected from unauthorized disclosure after chip authentication. This is done by using an encrypted communication channel, which is based on Secure Messaging provided by **F.Identification_Authentication**.

The SFR **FDP_UIT.1/MRTD** requires the transmitting and receiving data protected from modification, deletion, insertion and replay after chip authentication. This is done by using an protected communication channel. This channel is based on Secure Messaging provided by **F.Identification_Authentication**. A send sequence counter makes each command unique while the authenticity method makes it possible to detect modifications.

The SFR **FMT_SMF.1** requires security management functions for initialization, personalization and configuration. This is done by **F.Management**: the initialization and pre-personalization agent performs the initialization and configures the file layout in phase 2 and the personalization agent performs the personalization in phase 3.

The SFR **FMT_SMR.1** requires the maintenance of roles. The roles are managed by **F.Identification_Authentication**.

The SFR **FMT_LIM.1** requires limited capabilities of test functions which is provided by **F.IC_CL** which controls what commands can be executed thereby preventing external usable test functions to do harm. The IC Dedicated Test Software only is available in the Test Mode.

The SFR **FMT_LIM.2** requires limited availabilities of test functions which is provided by **F.IC_CL** which controls what commands can be executed thereby preventing external usable test functions to do harm. The IC Dedicated Test Software only is available in the Test Mode.

The SFR **FMT_MTD.1/INI_ENA** requires writing of initialization data and pre-personalization data to the manufacturer. Writing of pre-personalization and installation data only by the manufacturer is enforced by **F.Access_Control**, which limits these operations to phase 2. In addition **F.IC_CL** stores this data in the User Read Only Area which cannot be changed afterwards.

The SFR **FMT_MTD.1/INI_DIS** requires only the personalization agent to be able to disable reading of the initialization data. This is provided by **F.Management** (personalization agent: "Changing the TOE into the end-usage mode for phase 4 where reading of the initialization data is prevented") and **F.Access_Control**.

The SFR **FMT_MTD.1/CVCA_INI** requires only pre- and personalization agent to be able to write initial Country Verifying Certification Authority public public key, initial Country Verifier Certification Authority certificate and initial date. This is provided by **F.Access_Control**.

The SFR **FMT_MTD.1/CVCA_UPD** requires only country verifier certification authority to be able to update Country Verifier Certification Authority public public key and Country Verifier Certification Authority certificate. This is provided by **F.Identification_Authentication** (properties of terminal authentication).

The SFR **FMT_MTD.1/DATE** requires only country verifier certification authority, document verifier and domestic extended inspection system to be able to modify the current date. This is provided by **F.Identification_Authentication** (properties of terminal authentication).

The SFR **FMT_MTD.1/KEY_WRITE** requires the personalization agent to be able to write the Document Basic Access Keys. This is provided by **F.Access_Control** allowing the personalization agent in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/CAPK** requires the personalization agent to be able to load the Chip Authentication Private Key. This is provided by **F.Access_Control** allowing the personalization agent in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/AAPK** requires the personalization agent to be able to load the Active Authentication Private Key. This is provided by **F.Access_Control** allowing the personalization agent in phase 3 to write all necessary data.

The SFR **FMT_MTD.1/KEY_READ** requires the Document Basic Access Keys, the Chip Authentication Private Key, the Active Authentication Private Key and the Personalization Agent Keys to never be readable. This is enforced by **F.Access_Control**, which does not allow reading of any key to any role.

The SFR **FMT_MTD.3** requires only secure values of the certificate chain are accepted for data of the Terminal Authentication Protocol and the Access Control. This is done by **F.Identification_Authentication** (Terminal Authentication properties).

The SFR **FPT_EMSEC.1** requires limiting of emanations. This is provided by **F.IC_CL** (special DES protection, general protection and software countermeasures against side channel attacks).

The SFR **FPT_FLS.1** requires failure detection and preservation of a secure state. The Control of Operating Conditions of **F.IC_CL** is directly designed for this SFR. It audits continually and reacts to environmental and other problems by bringing it into a secure state.

The SFR **FPT_TST.1** requires testing for (a) correct operation, (b) integrity of data and (c) integrity of executable code. **F.Verification** this testing. **F.IC_CL** tests all EEPROM and ROM content for integrity ("... able to correct a 1-bit error within each byte" / "... parity check").

The SFR **FPT_SEP.1** requires separation of TSF and Non-TSF data. **F.IC_CL** does protect the embedded software against test functions of the hardware ("... control of the CPU mode ...").

The SFR **FPT_RVM.1** requires enforcement functions to succeed. This is provided by **F.Access_Control** which enforces first the TSP and then allows execution of the protected functions only on success ("... which are only executed after this TSF allowed access").

The SFR **FPT_PHP.3** requires resistance to physical manipulation and probing. This is provided by **F.IC_CL** which is provided by the hardware to resist attacks ("The function F.PHY protects the TOE against manipulation ..." / "... construction which make reverse-engineering and tamper attacks more difficult").

7.2.3 Rationale for Assurance Measures

The coverage of the Assurance Requirements by the Assurance measures is a direct one-to-one mapping.

7.2.4 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 component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD's chip especially for the absence of unintended functionality.

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

The selection of the component AVA_MSU.3 provides a higher assurance of the security of the MRTD's usage especially in phase 3 "Personalization of the MRTD" and Phase 4 "Operational Use". It is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The minimal strength of function "high" was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfill the OT.Sens_Data_Conf and OT.Chip_Auth_Proof. This is consistent with the security objective OD.Assurance.

The selection of the component AVA_VLA.4 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, OT.Chip_Auth_Proof and OD.Assurance.

The component ADV_IMP.2 has the following dependencies

- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ALC_TAT.1 Well-defined development tools

All of these are met or exceeded in the EAL4 assurance package.
The component ALC_DVS.2 has no dependencies.
The component AVA_MSU.3 has the following dependencies

- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

All of these are met or exceeded in the EAL4 assurance package.
The component AVA_VLA.4 has the following dependencies

- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_IMP.1 Subset of the implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

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

7.2.5 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 forms 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 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 additional assurance components shows that the assurance requirements are mutually supportive and internally consistent as all (additional) 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. Furthermore the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7.2.6 Strength of Function Level Rationale

Due to the requirements of the ST the level for the strength of the TOE's security functional requirements is claimed as SOF-high. The TOE is considered as a product with critical security mechanisms which only have to be defeated by attackers possessing a high level of expertise, opportunity and resources, and whereby successful attack is judged beyond normal practicability.

7.3 Rationale for PP Claims

This security target is conformant to the claimed Protection Profile BSI-PP-0026. Additionally, the Active Authentication Mechnism is included in the TOE. This implies the below described augmentations:

1. Addition of new TOE Objectives
   - OT.Active_Auth_Proof
2. Addition of new IT Environment Objectives
   - OE.Active_Auth_Key_MRTD
3. Addition of new SFRs for the TOE
   - FCS_COP.1/RSA_MRTD
   - FIA_API.1/AA
   - FMT_MTD.1/AAPK
4. Extension of existing SFRs for the TOE
   - FMT_MTD.1/KEY_READ: Inclusion of the Active Authentication Private Key
   - FPT_EMSEC.1: Inclusion of the Active Authentication Private Key
5. Addition of new IT environment SFRs
   - FCS_COP.1.1/RSA_BT

6. Extension of IT environment SFRs

    - FIA_UAU.4/BT: Inclusion of the Active Authentication Mechanism

For dependencies see Table 7.4

7.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the NXP Chip P5CD080 [1].

7.4.1 Relevance of Hardware TSFs

Table 7.6 shows the relevance of the hardware security functions for the composite security target.

	Relevant	Not relevant
Hardware TSFs [27]		
F.RNG: Random Number Generator	x	
F.HW_DES: Triple-DES Co-processor	x	
F.HW_AES: AES Co-processor		x
F.OPC: Control of Operating Conditions	x	
F.PHY: Protection against Physical Manipulation	x	
F.LOG: Logical Protection	x	
F.COMP: Protection of Mode Control	x	
F.MEM_ACC: Memory Access Control	x	
F.SFR_ACC: Special Function Register Access Control	x	
Crypto Library TSFs [1]		
F.AES: AES Cryptographic Function		x
F.DES: DES Cryptographic Function		x
F.RSA_encrypt: RSA Implementation for Data En- and Decryption	x	
F.RSA_sign: (CRT-)RSA Impl. for Signature Generation and Verification		x
F.RSA_public: RSA Implementation for Computation of a Public Key		x
F.ECC_GF_p_ECDSA: ECC Signature Generation and Verification Functions	x	
F.ECC_GF_p_DH_KeyExch: Diffie Hellman Key Exchange Functions	x	
F.RSA_KeyGen: Functions to Generate RSA Key Pairs		x
F.ECC_GF_p_KeyGen: Functions for ECC over GF(p) Key Generation		x
F.SHA: Functions for Secure Hash Algorithms SHA-1, -224 and -256		x
F.RNG_Access: Implementation of Software RNG		x
F.Object_Reuse: Internal Security Measures to Clear Memory after Usage	x	
F.COPY: Functionality to Copy Memory Content Protected Against Side Channel Attacks		x
F.LOG: Logical Protection (Identical to Hardware TSF)	x	

Table 7.6: Relevance of Hardware TSFs for Composite ST

F.HW_AES, F.AES, F.DES, F.RSA_sign, F.RSA_public, F.RSA_KeyGen, F.ECC_GF_p_KeyGen, F.SHA, F.RNG_Access and F.COPY are not relevant. F.HW_AES and F.AES, F.DES, F.RSA_public, F.RSA_KeyGen, F.ECC_GF_ p_KeyGen and F.RNG_Access are not used at all, for F.RSA_sign and F.SHA own software is used and, as no secrets are copied, F.COPY is not necessary.

7.4.2 Compatibility: TOE Security Environment

Assumptions

The following list shows that neither assumptions of the TOE nor of the hardware have any

conflicts between each other. They are either not relevant for this Security Target or are covered by appropriate Security Objectives.

- Assumptions of the TOE
  - A.Pers_Agent (Personalization of the MRTD's chip): No conflict
  - A.Insp_Sys_Inspection (Systems for global interoperability): No conflict
  - A.Signature_PKI (PKI for Passive Authentication): No conflict
  - A.Auth_PKI (PKI for Inspection Systems): No conflict
- Assumptions of the hardware
  - A.Process-Card (Protection during Packaging, Finishing and Personalization): Not relevant
  - A.Plat-Appl (Usage of Hardware Platform): Not relevant
  - A.Resp-Appl (Treatment of User Data): Covered by Security Objective OT.Prot_Inf_Leak
  - A.Check-Init (Check of initialization data by the Smartcard Embedded Software): Covered by Security Objective OT.Identification
  - A.Key-Function (Usage of Key-dependent Functions): Covered by Security Objective OT.Prot_Inf_Leak

Threats

The Threats of the TOE and the hardware can be mapped (see Table 7.7) or are not relevant. They show no conflict between each other.

- Threats of the TOE
  - T.Chip_ID (Identification of MRTD's chip): No conflict
  - T.Skimming (Skimming the logical MRTD): No conflict
  - T.Read_Sensitive_Data (Read the sensitive biometric reference data): No conflict
  - T.Forgery (Forgery of data on MRTD's chip): No conflict
  - T.Counterfeit (MRTD's chip): No conflict
  - T.Abuse-Func (Abuse of Functionality): Matches T.Abuse-Func of the hardware ST
  - T.Information_Leakage (Information Leakage from MRTD's chip): Matches T.Leak-Inherent and T.Leak-Forced of the hardware ST
  - T.Phys-Tamper (Physical Tampering): Matches T.Phys-Probing and T.Phys-Manipulation of the hardware ST
  - T.Malfunction (Malfunction due to Environmental Stress): Matches T.Malfunction of the hardware ST

- Threats of the hardware
  - T.Leak-Inherent (Inherent Information Leakage): Matches T.Information_Leakage of the TOE ST
  - T.Phys-Probing (Physical Probing): Matches T.Phys-Tamper of the TOE ST
  - T.Malfunction (Malfunction due to Environmental Stress): Matches T.Malfunction of the TOE ST
  - T.Phys-Manipulation (Physical Manipulation): Matches T.Phys-Tamper of the TOE ST
  - T.Leak-Forced (Forced Information Leakage): Matches T.Information_Leakage of the TOE ST
  - T.Abuse-Func (Abuse of Functionality): Matches T.Abuse-Func of the TOE ST
  - T.RND (Deficiency of Random Numbers): Matches T.Abuse-Func of the TOE ST

	T.Abuse-Func	T.Information_Leakage	T.Phys-Tamper	T.Malfunction
T.Leak-Inherent		x		
T.Phys-Probing			x	
T.Malfunction				x
T.Phys-Manipulation			x	
T.Leak-Forced		x		
T.Abuse-Func	x			
T.RND	x			

Table 7.7: Mapping of hardware to TOE Threats

Organizational Security Policies

The Organizational Security Policies of the TOE and the hardware have no conflicts between each other. They are shown in the following list.

- Organizational Security Policies of the TOE
  - P.Manufact (Manufacturing of the MRTD's chip): Covers P.Process-TOE of the hardware ST

  - P.Personalization (Personalization of the MRTD by issuing State or Organization only): Not applicable
  - P.Personal Data (Personal data protection policy): Not applicable
  - P.Sensitive Data (Privacy of sensitive biometric reference data): Not applicable

- Organizational Security Policies of the hardware
  - P.Add-Components (Additional Specific Security Components): Not applicable
  - P.Process-TOE (Protection during TOE Development and Production): Covered by P.Manufact of the TOE ST
  - P.Add-Func (Additional Specific Security Functionality): Not applicable

Security Objectives

The Security Objectives of the TOE and the hardware can be mapped (see Table 7.8) or are not relevant. They show no conflict between each other.

- Security Objectives for the TOE
  - OT.AC_Pers (Access Control for Personalization of logical MRTD): No conflicts
  - OT.Data_Int (Integrity of personal data): No conflicts
  - OT.Data_Conf (Confidentiality of personal data): No conflicts
  - OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data): No conflicts
  - OT.Identification (Identification and Authentication of the TOE): Matches O.Identification of the hardware ST
  - OT.Chip_Auth_Proof (Proof of MRTD's chip authenticity): No conflicts
  - OT.Prot_Abuse-Func (Protection against Abuse of Functionality): Matches O.Abuse-Func, O.MEM_ACCESS, O.SFR_ACCESS and O.CONFIG of the hardware ST
  - OT.Prot_Inf_Leak (Protection against Information Leakage): Matches O.Leak-Inherent and O.Leak-Forced of the hardware ST
  - OT.Prot_Phys-Tamper (Protection against Physical Tampering): Matches O.Phys-Probing and O.Phys-Manipulation of the hardware ST
  - OT.Prot_Malfunction (Protection against Malfunctions): Matches O.Malfunction of the hardware ST
  - OT.Active_Auth_Proof (Proof of MRTD's chip authenticity): No conflicts

- Security Objectives for the hardware
  - O.Leak-Inherent (Protection against Inherent Information Leakage): Covered by OT.Prot_Inf_Leak of the TOE ST

  - O.Phys-Probing (Protection against Physical Probing): Covered by OT.Prot_Phys-Tamper of the TOE ST
  - O.Malfunction (Protection against Malfunctions): Covered by OT.Prot_Malfunction of the TOE ST
  - O.Phys-Manipulation (Protection against Physical Manipulation): Covered by OT.Prot_Phys-Tamper of the TOE ST
  - O.Leak-Forced (Protection against Forced Information Leakage): Covered by OT.Prot_Inf_Leak of the TOE ST
  - O.Abuse-Func (Protection against Abuse of Functionality): Covered by OT.Prot_Abuse-Func of the TOE ST
  - O.Identification (TOE Identification): Covered by OT.Identification of the TOE ST
  - O.RND (Random Numbers): No conflicts
  - O.HW_DES3 (Triple DES Functionality): : No conflicts
  - O.HW_AES (AES Functionality): Not relevant
  - O.MF_FW (MIFARE Firewall): Not relevant
  - O.MEM_ACCESS (Area based Memory Access Control): Covered by OT.Prot_Abuse-Func of the TOE ST
  - O.SFR_ACCESS (Special Function Register Access Control): Covered by OT.Prot_Abuse-Func of the TOE ST
  - O.CONFIG (Protection of configuration data): Covered by OT.Prot_Abuse-Func of the TOE ST

- Security Objectives of the crypto library
  - O.AES (AES Functionality): Not relevant
  - O.DES3 (Triple DES Functionality): Not relevant for SW DES, else see O.HW_DES3
  - O.RSA (RSA Functionality): : No conflicts
  - O.RSA_PubKey (RSA Public Key Computation): Not relevant
  - O.RSA_KeyGen (RSA Public Key Pair Generation): Not relevant
  - O.ECC (ECC Signature Creation and Verification): : No conflicts
  - O.ECC_DHKE (ECC Diffie-Hellman Key Exchange): : No conflicts
  - O.ECC_KeyGen (ECC Key Pair Generation): Not relevant
  - O.SHA (SHA algorithms): Not relevant
  - O.COPY (Copy Memory Content Protected against Side Channel Attacks): Not relevant
  - O.REUSE (Memory Resources cannot be Disclosed to Subsequent Users): Covered by OT.Prot_Abuse-Func of the TOE ST

	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
O.Leak-Inherent			x		
O.Phys-Probing				x	
O.Malfunction					x
O.Phys-Manipulation				x	
O.Leak-Forced			x		
O.Abuse-Func		x			
O.Identification	x				
O.MEM_ACCESS		x			
O.SFR_ACCESS		x			
O.CONFIG		x			
O.REUSE		x			

Table 7.8: Mapping of hardware to TOE Security Objectives

Security Requirements

The relevant Security Requirements of the TOE and the hardware can be mapped (see Table 7.9) or are not relevant. They show no conflict between each other.

- Relevant Security Requirements of the TOE
  - FAU_SAS.1 (Audit storage) Matches FAU_SAS.1 of the hardware ST
  - FCS_CKM.1/KDF_MRTD (Cryptographic key generation - Key Derivation Function by the MRTD): No conflicts
  - FCS_CKM.1/DH_MRTD (Cryptographic key generation - Diffie-Hellman Keys by the MRTD): Matches FCS_COP.1 [ECC_DHKE] of the hardware ST
  - FCS_CKM.4 (Cryptographic key destruction - MRTD): No conflicts
  - FCS_COP.1/SHA_MRTD (Cryptographic operation - Hash for Key Derivation by MRTD): Matches FCS_COP.1 [SHA]of the hardware ST
  - FCS_COP.1/TDES_MRTD (Cryptographic operation - Encryption / Decryption Triple DES): Matches FCS_COP.1 [DES] of the hardware ST
  - FCS_COP.1/MAC_MRTD (Cryptographic operation - Retail MAC): Matches FCS_COP.1 [DES] of the hardware ST

- FCS_COP.1/SIG_VER (Cryptographic operation - Signature verification by MRTD): Matches FCS_COP.1 [ECC_GF_p] of the hardware ST
- FCS_COP.1/RSA_MRTD (Cryptographic operation - Signature creation by MRTD): Matches FCS_COP.1 [RSA_encrypt] of the hardware ST
- FCS_RND.1/MRTD (Quality metric for random numbers): Matches FCS_RND.1 of the hardware ST
- Class FIA (Identification and Authentication): No conflicts
- FDP_ACC.1 (User Data Protection - Subset access control): Matches FDP_ACC.1 of the hardware ST
- FDP_ACF.1 (User Data Protection - Security attribute based access control): Matches FDP_ACF.1 of the hardware ST
- Other Class FDP (User Data Protection): No conflicts
- FMT_SMF.1 (Specification of Management Functions): Matches FMT_SMF.1 of the hardware ST
- FMT_LIM.1 (Limited capabilities): Matches FMT_LIM.1 of the hardware ST
- FMT_LIM.2 (Limited availability): Matches FMT_LIM.2 of the hardware ST
- FMT_MTD.1/INI_ENA (Management of TSF data - Writing of Initialization Data and Prepersonalization Data): Matches FPT_SEP.1 [CONF] of the hardware ST
- FMT_MTD.1/INI_DIS (Management of TSF data - Disabling of Read Access to Initialization Data and Pre-personalization Data): Matches FPT_SEP.1 [CONF] of the hardware ST
- Other Class FMT (Management of TSF data): No conflicts
- FPT_EMSEC.1 (TOE Emanation): Matches FDP_ITT.1 and FPT_ITT.1 of the hardware ST
- FPT_FLS.1 (Failure with preservation of secure state): Matches FPT_FLS.1, FRU_FLT.2 and FPT_PHP.3 of the hardware ST
- FPT_TST.1 (TSF testing): Matches FRU_FLT.2 and FPT_TST.2 of the hardware ST
- FPT_PHP.3 (Resistance to physical attack): Matches FRU_FLT.2 and FPT_PHP.3 of the hardware ST
- FPT_RVM.1 (Non-bypassability of the TSP): No conflicts
- FPT_SEP.1 (TSF domain separation) Matches FPT_SEP.1 of the hardware ST

- Security Requirements of the hardware
  - FAU_SAS.1 (Audit storage): Covered by FAU_SAS.1 of the TOE ST
  - FCS_COP.1 [AES] (Cryptographic operation - AES): Not relevant
  - FCS_COP.1 [DES] (Cryptographic operation - DES): Covered by FCS_COP.1/ TDES_MRTD and FCS_COP.1/MAC_MRTD of the TOE ST
  - FCS_RND.1 (Quality metric for random numbers): Covered by FCS_RND.1/MRTD of the TOE ST

- FDP_ACC.1 [MEM] and [SFR] (Subset access control): Covered by FDP_ACC.1 of the TOE ST
- FDP_ACF.1 [MEM] and [SFR] (Subset access control): Covered by FDP_ACF.1 of the TOE ST
- FDP_ITT.1 (Basic internal transfer protection): Covered by FPT_EMSEC.1 of the TOE ST
- FDP_IFC.1 (Subset information flow control): Covered by FPT_EMSEC.1 of the TOE ST
- FMT_SMF.1 (Specification of Management Functions): Covered by FMT_SMF.1 of the TOE ST
- FMT_LIM.1 (Limited capabilities): Covered by FMT_LIM.1 of the TOE ST
- FMT_LIM.2 (Limited availability): Covered by FMT_LIM.2 of the TOE ST
- FMT_MSA.3 [MEM] and [SFR] (Static attribute initialization): No conflicts
- FMT_MSA.1 [MEM] and [SFR] (Management of security attributes): No conflicts
- FPT_FLS.1 (Failure with preservation of secure state): Covered by FPT_FLS.1 of the TOE ST
- FPT_ITT.1 (Basic internal TSF data transfer protection): Covered by FPT_EMSEC.1 of the TOE ST
- FPT_PHP.3 (Resistance to physical attack): Covered by FPT_FLS.1 and FPT_PHP.3 of the TOE ST
- FPT_SEP.1 [PP] (TSF domain separation): Covered by FPT_SEP.1 of the TOE ST
- FPT_SEP.1 [CONF] (TSF domain separation): Covered by FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS of the TOE ST
- FRU_FLT.2 (Limited fault tolerance): Covered by FPT_FLS.1, FPT_TST.1 and FPT_PHP.3 of the TOE ST

- Security Requirements of the crypto library
  - FCS_COP.1 [SW-AES] (Cryptographic operation): Not relevant
  - FCS_COP.1 [SW-DES] (Cryptographic operation): Not relevant
  - FCS_COP.1 [RSA_encrypt] (Cryptographic operation - RSA encryption and decryption): Covered by FCS_COP.1/RSA_MRTD of the TOE ST
  - FCS_COP.1 [RSA_public] (Cryptographic operation - RSA public key computation): Not relevant
  - FCS_COP.1 [RSA_sign] (Cryptographic operation - RSA signature generation and verification): Not relevant
  - FCS_COP.1 [ECC_GF_p] (Cryptographic operation (ECC over GF(p) signature generation and verification)): Covered by FCS_COP.1/SIG_VER of the TOE ST
  - FCS_COP.1 [ECC_DHKE] (Cryptographic operation (ECC Diffie-Hellman key exchange)): Covered by FCS_CKM.1/DH_MRTD of the TOE ST

- FCS_COP.1 [SHA] (Cryptographic operation - SHA-1, SHA-224 and SHA-256: Covered by FCS_COP.1/SHA_MRTD of the TOE ST
- FCS_CKM.1 [RSA] (Cryptographic key generation - RSA): Not relevant
- FCS_CKM.1 [ECC_GF_p] (Cryptographic key generation - ECC over GF(p)): Covered by FCS_CKM.1/DH_MRTD of the TOE ST
- FDP_RIP.1 (Subset residual information protection): No conflict
- FDP_ITT.1 [COPY] (Basic internal transfer protection): No conflict
- FPT_ITT.1 [COPY] (Basic internal TSF data transfer protection): No conflict
- FCS_RND.2 (Random number generation (SW)): Not relevant
- FPT_TST.2 (Subset TOE security testing): Covered by FPT_TST.1 of the TOE ST

	FAU_SAS.1	FCS_CKM.1/DH_MRTD	FCS_COP.1/SHA_MRTD	FCS_COP.1/TDES_MRTD	FCS_COP.1/MAC_MRTD	FCS_COP.1/SIG_VER	FCS_COP.1/RSA_MRTD	FCS_RND.1/MRTD	FDP_ACC.1	FDP_ACF.1	FMT_SMF.1	FMT_LIM.1	FMT_LIM.2	FMT_MTD.1/INI_ENA	FMT_MTD.1/INI_DIS	FPT_EMSEC.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3	FPT_SEP.1
FAU_SAS.1	x																			
FCS_COP.1 [DES]				x	x															
FCS_RND.1								x												
FDP_ACC.1									x											
FDP_ACF.1										x										
FDP_ITT.1																x				
FDP_IFC.1																x				
FMT_SMF.1											x									
FMT_LIM.1												x								
FMT_LIM.2													x							
FPT_FLS.1																	x			
FPT_ITT.1																x				
FPT_PHP.3																	x		x	
FPT_SEP.1																				x
FPT_SEP.1 [CONF]														x	x					
FRU_FLT.2																	x	x	x	
FCS_COP.1 [RSA_encrypt]							x													
FCS_COP.1 [ECC_GF_p]						x														
FCS_COP.1 [ECC_DHKE]		x																		
FCS_COP.1 [SHA]			x																	
FCS_CKM.1 [ECC_GF_p]		x																		
FPT_TST.2																		x		

Table 7.9: Mapping of of hardware to TOE Security SFRs

Assurance Requirements

The level of assurance of the TOE is EAL 4 augmented with

- ADV_IMP.2
- ALC_DVS.2
- AVA_MSU.3

- AVA_VLA.4

The chosen level of assurance of the hardware is EAL 5 augmented with

- ALC_DVS.2
- AVA_MSU.3
- AVA_VLA.4

This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

7.4.3 Conclusion

Overall no contradictions between the Security Targets of the TOE and the hardware can be found.

Chapter 8

Glossary and Acronyms

Active Authentication Security mechanism defined in [3] 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 ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1 [13], section B.2.7).

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 Access Control Security mechanism defined in [3] by which means the MRTD's chip proves and the Inspection System protects their communication by means of Secure Messaging with 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 themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.

Biographical data (biodata) The personalized details of the bearer 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. [10]

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 Inspection System 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 unauthorized copy or reproduction of a genuine security document made by whatever means. [10]

Country Signing CA Certificate (CCSCA) Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority 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 Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD. It is 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 [3], Annex E.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 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 [3]. 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 (SOD) A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [3]

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 low attack potential reading the communication between the MRTD's chip and the Inspection System to gain the data on the MRTD's chip.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [28]

Extended Access Control Security mechanism identified in [3] by which means the MRTD's chip (i) verifies the authentication of the Inspection Systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference

data during their transmission to the Inspection System by Secure Messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication 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 Authentication Mechanism.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [10]

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 utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all MRTDs. [28]

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.

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. [10]

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. [28]

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. [28]

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). [2]

Issuing State The Country issuing the MRTD. [2]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [2]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD Data of the MRTD holder stored according to the Logical Data Structure [2] 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
5. the other data according to LDS (EF.DG5 to EF.DG16)

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)
3. fingerprint image(s) and/or iris image(s) (optional)

Machine readable travel document (MRTD) Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [2]

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. [2]

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. [2]

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. [10]

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 [2]
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16)
- the TSF Data including the definition the authentication data but except the authentication data itself.

MRTD Basic Access Control Mutual authentication protocol followed by Secure Messaging between the Inspection System and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

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

MRTD's Chip A contactless integrated circuit chip complying with ISO/IEC 14443 [11] and programmed according to the Logical Data Structure as specified by ICAO, [29] 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. [10]

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 Authentication Key Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT, FIA_UAU.6/BT and FIA_API.1/SYM_PT 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/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.

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 Data Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.

Pre-personalized MRTD's chip MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.

Receiving State The Country to which the MRTD holder is applying for entry. [2]

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. [10]

Secure messaging in encrypted mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [30].

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 Verifier 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 organization which may be used by the rightful holder for international travel. [28]

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 [13]).

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

User data Data created by and for the user that does not affect the operation of the TSF (CC part 1 [13]).

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. [28]

Verification data Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

BIS	Basic Inspection System
CC	Common Criteria
EIS	Extended Inspection System
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functions

Bibliography

[1] NXP. Security Target 'Secured Crypto Library on the P5CD080V0B'. BSI-DSZ-CC-0417-2008-MA-02, Rev. 1.3.2. NXP, 2010-05-10.

[2] ICAO. Technical Report: Development of a Logical Data Structure - LDS - for optional Capacity Expansion Technologies. International Civil Aviation Organization, 2004-05.

[3] ICAO. Technical Report: PKI for Machine Readable Travel Documents offering ICC read-only access. V1.1. International Civil Aviation Organization, 2004-10.

[4] TR-03110, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents Extended Access Control (EAC), Version 1.11, BSI, 2008.

[5] MaskTech GmbH. MTCOS Standard & Pro V2.1: Part 1 - Filesystem and Security Architecture, Version 1.02, 2009-05-18.

[6] MaskTech GmbH. MTCOS Standard & Pro V2.1: Part 2 - Basic Access Control and Secure Messaging, Version 1.00, 2008-04-08.

[7] MaskTech GmbH. MTCOS Pro V2.1 : Part 3 - Digital Signature, Version 1.00, 2008-04-02.

[8] MaskTech GmbH. MTCOS Standard & Pro V2.1: Part 5 - Advanced Security Mechanisms Extended Access Control, Version 1.01, 2008-06-20.

[9] MTCOS Pro 2.1 EAC/P5CD080/V2 User Guidance, Version 1.2, G. Schürer, 2010-01-20.

[10] ICAO. Security Standards for Machine Readable Travel Documents, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, ANNEX to Section III. International Civil Aviation Organization, 2003.

[11] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Multipart Standard, ISO/IEC, 2000/2001.

[12] ISO/IEC 7816:2004-2007, Information technology – Identification cards – Integrated circuit(s) cards with contacts – Multipart Standard, ISO/IEC, 2004-2007.

[13] CCMB-2005-08-001, Version 2.3, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2005-08.

[14] CCMB-2005-08-002, Version 2.3, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Common Criteria Maintenance Board, 2005-08.

[15] E. Rescorla. Diffie-Hellman Key Agreement Method, RFC (Request for Comments) series (online). Internet Engineering Task Force, 1999.

[16] ISO/IEC 15946:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Multipart Standard, ISO/IEC, 2002.

[17] FIPS PUB 140-2, Security Requirements for Cryprographic Modules, NIST, 2001-05.

[18] FIPS PUB 180-2, Secure Hash Standard, NIST, 2002-08.

[19] FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), NIST, 1999-10.

[20] ISO/IEC9797:1999, 2002, Information technology – Security techniques – Message Authentication Codes (MACs) – Multipart Standard, ISO/IEC, 1999, 2002.

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

[22] AIS 20, Version 1.0, Anwendungshinweise und Interpretationen zum Schema (AIS) – Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI, 1999-12-02.

[23] ISO/IEC11568-2:2005, Banking – Key Management (Retail) – Part 2: Symmetric Ciphers, their Key Management and Life Cycle, ISO/IEC, 2005.

[24] ISO/IEC9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO/IEC, 1999.

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

[26] BSI-PP-0026, Version 1.2, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application, Extended Access Control', BSI, 2007-11-19.

[27] NXP. NXP Semiconductors Documentation: Security Target Lite - P5CD080/P5CN080/P5CC080/P5CC073V0B. BSI-DSZ-CC-0410-2007-MA-07, Rev. 1.7. NXP, 2009-09-28.

[28] ICAO. Biometrics Deployment of Machine Readable Travel Documents - Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using Machine Readable Travel Documents. ICAO TAG MRTD/NTWG. International Civil Aviation Organization, 2003.

[29] ICAO. Facilitation (FAL) Division, twelfth session, Cairo. International Civil Aviation Organization, 10-2004.

[30] ISO/IEC 7816-4: 2005, Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange, ISO/IEC, 2005-01.