Security Target – lite

Machine Readable Travel Document with "ICAO Application", Extended Access Control MTCOS Pro 2.1 EAC/ST23YR80

MASKTECH INTERNATIONAL GMBH

Document number: BSI-DSZ-CC-0664, ST – lite, Version 1.4

Created by: Gudrun Schürer

Date: 2011-02-10

Signature:

Released by Management:

Date:

Signature:

Change history

Version	Date	Reason	Remarks
1.0	2011-01-18	Public version based on BSI-DSZ-CC-0664/ST	
1.1	2011-01-31	Final public version	
1.2	2011-02-01	Minor correction	
1.3	2011-02-07	Inclusion of ECC Curve parameter references	
1.4	2011-02-10	Some final changes	

Contents

Chapter 1

ST Introduction (ASE_INT.1)

1.1 ST Reference and TOE reference

Title	Security Target – Machine Readable Travel Document with ICAO Application, Extended Access Control (ST-MRTD EAC)
Version	1.4, 2011-02-10
Editors	Gudrun Schürer
Compliant to	Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10, BSI-CC-PP-0056
CC Version	3.1 (Revision 3)
Assurance Level	The assurance level for this ST is EAL4 augmented
TOE name	MTCOS Pro 2.1 EAC/ST23YR80, operation system for secure passports
TOE Hardware	ST Microelectronics SB23YR80B, dual interface Smartcard IC
TOE version	MTCOS Pro 2.1 EAC
Keywords	ICAO, machine readable travel document, extended access control

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control, Extended Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [1].

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816 [2]. 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 ST Microelectronics SB23YR80B secure dual-interface controller, which is directly derived from the dual smartcard IC ST23YR80B by the addition of the public key cryptographic library NesLib SB. SB23YR80B is certified

according to CC EAL6 augmented (ANSSI-2010/02 [3] compliant to the Protection Profile BSI-PP-0035 [4]). This means, that the TOE consists of software and hardware.

TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [5] and providing Basic Access Control, Active Authentication and Extended Access Control according to the ICAO documents [1, 6] and Chip Authentication according to the technical report TR-03110 [7].

The TOE comprises of

- the circuitry of the MRTD's chip (the integrated circuit, IC)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- the IC Embedded Software (operating system)
- the MRTD application
- the associated guidance documentation [8, 9, 10, 11, 12]

The TOE is based on ISO/IEC 7816 [2] 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. For further details concerning BAC, see the Security Target – lite of BSI-DSZ-CC-0671 [13].

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 [6] for Basic Access Control
- Extended Access Control (EAC) as specified in TR-03110 [7]
- Active Authentication as specified in TrPKI [6]
- Contactless communication according to ISO/IEC 14443 [14]
- Protection of the privacy of the passport holder with functions like random UID and Basic Access Control

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 [5] 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 [5] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

1. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1)
2. the digitized portraits (EF.DG2)
3. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
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) [1]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication

of the MRTD's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [1]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This Security Target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This Security Target addresses the Chip Authentication described in [7] as an alternative or as an addition to the Active Authentication stated in [1].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by BSI-CC-PP-0056 [15] as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' BSI-CC-PP-0055 [16]. Due to the fact that [16] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately. The evaluation and certification process is carried out contemporaneous to the current process as a re-certification.

For BAC, the Inspection System (i) reads optically the MRTD, (ii) authenticates itself as Inspection System by means of Document Basic Access Keys. After successful authentication of the Inspection System the MRTD's chip provides read access to the logical MRTD by means of private communication (Secure Messaging) with this Inspection System according to [1], normative appendix 5.

The Security Target requires the TOE to implement the Chip Authentication defined in [7] and the Active Authentication described in [6]. Both protocols provide evidence of the MRTD's chip authenticity where the Chip Authentication prevents data traces described in [1], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the Inspection System communicates by means of Secure Messaging established by Basic Access Control, (ii) the Inspection System reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the Inspection System generates 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. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The Security Target requires the TOE to implement the Extended Access Control as defined in [7]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol and (ii) the Terminal Authentication Protocol. The Chip Authentication Protocol (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the

issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

TOE Life Cycle

The TOE life cycle is described in terms of the four life cycle phases. With respect to [4], the TOE life cycle is additionally subdivided into 7 step.

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

(**Step 2**) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

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

Phase 2: Manufacturing (**Step 3**) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

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

(**Step 4**) See **Inlay production** below

(**Step 5**) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization Data. The Initialization and Pre-personalization described in this step is performed by SmartTrac, Thailand (see [17]) and MASKTECH INTERNATIONAL.

Note: For file based operating systems, the creation of the application implies the creation of MF and ICAO.DF.

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.

(**Inlay production**) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book. The inlay production including the application of the antenna is **NOT** part of the TOE and takes part after the delivery.

Phase 3: Personalization of the MRTD (**Step 6**) 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) 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 [1] 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.

Phase 4: Operational Use (**Step 7**) 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.

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

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

Chapter 2

Conformance Claims (ASE_CCL.1)

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1 Revision 3, July 2009 [18]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; CCMB-2009-07-002, Version 3.1 Revision 3, July 2009 [19]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1 Revision 3, July 2009 [20]

as follows

- Part 2 extended
- Part 3 conformant

The

- Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1 Revision 3, July 2009 [21]

has to be taken into account.

2.2 PP Reference

The conformance of this ST to the Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.10, BSI-CC-PP-0056 [15] is claimed.

2.3 PP Additions

Active Authentication based on ICAO PKI v1.1 [6] has been added. This implies the following augmentations:

1. Extension of existing Assumptions for the TOE
   - A.Pers_Agent: Inclusion of Active Authentication
   - A.Insp_Sys: Inclusion of Active Authentication
2. Addition of new TOE Objectives
   - OT.Active_Auth_Proof
3. Addition of new IT Environment Objectives
   - OE.Active_Auth_Key_MRTD
4. Addition of new SFRs for the TOE
   - FCS_COP.1/RSA_MRTD_AA
   - FIA_API.1/AA
   - FMT_MTD.1/AAPK
5. Extension of existing SFRs for the TOE
   - FMT_MTD.1/KEY_READ_AA: Inclusion of the Active Authentication Private Key
   - FPT_EMSEC.1/AA: Inclusion of the Active Authentication Private Key

Table 6.3 takes the dependencies of the SFRs into account.

2.4 Package Claim

The assurance level for the TOE is CC EAL4 augmented augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [20].

2.5 Conformance rationale

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

Chapter 3

Security Problem Definition (ASE_SPD.1)

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 [5]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the Inspection System for the Chip Authentication and the Active Authentication Public Key (EF.DG15) for Active Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons the 'ICAO Doc 9303' [1] specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

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

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the MRTD's chip The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove 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 [5].

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

Document Verifier The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in 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 additionally the Chip Authentication Mechanism. The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates. 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 manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD.

Note: An attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this ST since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [16]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 as well as EF.SOD and EF.COM.

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

3.2 Assumptions

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

A.MRTD_Manufact (MRTD manufacturing on steps 4 to 6) It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery (MRTD delivery during steps 4 to 6) Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

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

A.Pers_Agent (Personalization of the MRTD's chip) The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) and Active Authentication Public Key (EF.DG15)f 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 [6]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes Secure Messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. 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 securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

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

3.3 Threats

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

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

T.Read_Sensitive_Data (Read the sensitive biometric reference data)

Adverse action An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

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

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

T.Forgery (Forgery of data on MRTD's chip)

Adverse action An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

Threat agent Having high attack potential, being in possession of one or more legitimate MRTDs.

Asset Authenticity of logical MRTD data.

T.Counterfeit (MRTD's chip)

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

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

Threat agent Having high attack potential, being in possession of one or more legitimate MRTDs.

Asset Authenticity of logical MRTD data.

The TOE shall avert the threats as specified below.

T.Abuse-Func (Abuse of Functionality)

Adverse action An attacker may use functions of the TOE which shall not be used in "Operational Use" phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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

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

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality of logical MRTD and TSF data.

T.Phys-Tamper (Physical Tampering)

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

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Malfunction (Malfunction due to Environmental Stress)

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

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

Threat agent Having high attack potential, being in possession of a legitimate MRTD.

Asset Confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

3.4 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 [18]).

P.BAC-PP (Fulfillment of the Basic Access Control Protection Profile) The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [1] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' [16] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

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

P.Manufact (Manufacturing of the MRTD's chip) The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

Chapter 4

Security Objectives (ASE_OBJ.2)

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

4.1 Security Objectives for the TOE

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

OT.AC_Pers (Access Control for Personalization of logical MRTD) The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [5] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Note: The OT.AC_Pers implies that

1. the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization
2. the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int (Integrity of personal data) The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

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

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

OT.Chip_Auth_Proof (Proof of MRTD's chip authenticity) The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [7]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

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) After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak (Protection against Information Leakage) The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE

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

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.

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

OT.Active_Auth_Proof (Proof of MRTD's chip authenticity) The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [6]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

4.2 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.MRTD_Manufact (Protection of the MRTD Manufacturing) Appropriate functionality testing of the TOE shall be used in step 4 to 6.

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

OE.MRTD_Delivery (Protection of the MRTD delivery) Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- Non-disclosure of any security relevant information
- Identification of the element under delivery
- Meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment)
- Physical protection to prevent external damage
- Secure storage and handling procedures (including rejected TOE's)
- Traceability of TOE during delivery including the following parameters:
  - Origin and shipment details
  - Reception, reception acknowledgment
  - Location material/information

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

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

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

OE.Pass_Auth_Sign (Authentication of logical MRTD by Signature) The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and organizations maintaining its authenticity and integrity. The issuing State or organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document 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 [5].

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

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

OE.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.

OE.BAC_PP (Fulfillment of the Basic Access Control Protection Profile) It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' [16]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

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 [6]. 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 CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all Inspection Systems.

OE.Prot_Logical_MRTD (Protection of data 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. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

OE.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.

4.3 Security Objective Rationale

The Active Authentication functionality (for better readability the Security Objectives in question are highlighted by an underline) is included in the *Security Objective Rationale*. The table 4.1 provides an overview for Security Objectives coverage.

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

Table 4.1: Security Objective Rationale (including Active Authentication)

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

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

The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the (i) the 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 Key(s) ac-

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

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

The threat **T.Forgery** “Forgery of data on MRTD’s chip” addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** “Integrity of personal data” and **OT.Prot_Phys-Tamper** “Protection against Physical Tampering”. The examination of the presented MRTD passport book according to **OE.Exam_MRTD** “Examination of the MRTD passport book” shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” and verified by the inspection system according **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. 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 Organization. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_MRTD** “MRTD Authentication Key”.

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE **OT.Prot_Abuse-Func** "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the "Operational Use" phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered. Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** "Personalization of logical MRTD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

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

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

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

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

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.Signature_PKI** "PKI for Passive Authentication"is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD** "Examination of the MRTD passport book".

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

Chapter 5

Extended Components Definition (ASE_ECD.1)

This Security Target uses the components defined in chapter 5 of BSI-CC-PP-0056 [15]. No other components are used.

Chapter 6

Security Requirements (ASE_REQ.2)

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 of the CC [18]. 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 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 filled in by the ST author are denoted as double-underlined text.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in chapter 8 or in the following table. The operations "write", "modify", "read" and " disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and " re-authenticate" are originally taken from [19]. The operation "load" is synonymous to "import" used in [19].

Definition of security attributes

Terminal authentication status

none (any Terminal) default role (i.e. without authorization after start-up)

CVCA roles defined in the certificate used for authentication (cf. [7], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA

DV (domestic) roles defined in the certificate used for authentication (cf. [7], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA

DV (foreign) roles defined in the certificate used for authentication (cf. [7], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA

IS roles defined in the certificate used for authentication (cf. [7], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA

Terminal Authorization none

DG4 (Iris) Read access to DG4: (cf. [7], A.5.1)

DG3 (Fingerprint) Read access to DG3: (cf. [7], A.5.1)

DG3 (Fingerprint) / DG4 (Iris) Read access to DG3 and DG4: (cf. [7], A.5.1)

Overview of the keys and certificates used in this ST

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. [7] 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 [22] or Elliptic Curve Diffie-Hellman according to ISO 15946 [23].

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.

Active Authentication Public Key Pair

The Active Authentication Public Key Pair (SK_{AA}, PK_{AA}) are used for Active Authentication according to TrPKI [6]. (Included in addition to EAC-PP to take the Active Authentication functionality into account.)

Active Authentication Public Key (PK_{AA})

The Active Authentication Public Key (PK_{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 (SK_{AA})

The Active 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.

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

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 [19] extended).

FAU_SAS.1 Audit storage

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

Note: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 *Manufacturing*. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 Class Cryptographic Support (FCS)

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2 [19]). The iterations are caused by different cryptographic key generation algorithms to be implemented and keys to be generated by the TOE.

FCS_CKM.1 Cryptographic key generation – Generation of Diffie-Hellman Keys by the TOE

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH and specified cryptographic key sizes 112 bits that meet the following: TR-03110 [7], Annex A.1

Note: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [7], sec. 3.1 and Annex A.1. This protocol is based on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [7], Annex A.1, [24] and [25] for details). The shared secret value is used to derive the Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [1], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC. The following curves are provided: NIST Curves P-224, P-256 and P-384 [26] and Brainpool brainpoolP224r1, brainpoolP256r1 and brainpoolP3204r1 [27].

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2 [19]).

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with the cryptographic key destruction method physical deletion of key value that meets the following: FIPS PUB 140-2 [28].

Note: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging (specified in BSI-CC-PP-055 [16]). The TOE shall destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC, and (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.

Cryptographic Operation (FCS_COP.1)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2 [19]). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	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 [29].

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SYM	The TSF shall perform Secure Messaging - encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key size 112 bit that meet the following: TR-03110 [7].

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

FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: TR-03110 [7].

Note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol according to the FCS_CKM.1. The Retail-MAC as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 (cf. [16]) is DES resp. two-key Triple-DES base.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-224 or SHA-256 and cryptographic key sizes 224, 256, 320 and 384 bits that meet the following: FIPS 180-2 [29].

Note: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4 (specified in BSI-CC-PP-0055 [16]). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge. The following curves are provided: NIST Curves P-224 and P-256 [26] and Brainpool brainpoolP224r1, brainpoolP256r1 and brainpoolP3204r1 [27].

FCS_COP.1/RSA_MRTD_AA Cryptographic operation – Signature creation by MRTD – AA

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ RSA_MRTD_AA	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA with SHA-1 and cryptographic key sizes 1536 bits that meet the following: ISO/IEC 9796-2:2002 [30].

(This SFR is defined in addition to BSI-CC-PP-0056 [15] to include the Active Authentication functionality.)

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 [19]).

FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet class P2 defined in AIS31 [31].

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

6.1.3 Class FIA Identification and Authentication

Note: Table 6.1 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6
Terminal Authentication Protocol	FIA_UAU.5
Active Authentication (specified in addition to BSI-CC-PP-0056 [15])	FIA_API.1/AA

Table 6.1: Overview on authentication SFR

Note the Chip Authentication Protocol as defined in BSI-CC-PP-0056 [15] includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [1] in order to gain access to the Chip Authentication Public Key in EF.DG14
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal

The BAC mechanism does not provide a security function on its own (nevertheless it is listed in table 6.1 for completeness). The Chip Authentication Protocol may be used independent of the Terminal Authentication Protocol. But if the Terminal Authentication Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol.

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2 [19]).

FIA_UID.1 Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow 1. to establish the communication channel 2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS 3. to carry out the Chip Authentication Protocol 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.

Note: In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer creates the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. BSI-CC-PP-0055 [16]) is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is a mandatory part within the Chip Authentication Protocol). After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2 [19]).

FIA_UAU.1 Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow 1. to establish the communication channel 2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS 3. to identify themselves by selection of the authentication key 4. to carry out the Chip Authentication Protocol 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.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2 [19]).

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

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

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

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2 [19]).

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1	The TSF shall provide 1. Terminal Authentication Protocol 2. Secure messaging in MAC-ENC mode 3. Symmetric Authentication Mechanism based on Triple-DES to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. The TOE accepts the authentication attempt as Personalization Agent by the following mechanism (a) the Terminal Authentication Protocol with Personalization Agent Keys 2. 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 3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the Secure Messaging established by the Chip Authentication Mechanism

Note: The Personalization Agent holds an asymmetric key pair for the Terminal Authentication Protocol. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2 [19]).

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS.

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

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended [19]).

FIA_API.1 Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol according to [7] to prove the identity of the TOE.

Note: This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [7]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [1], normative appendix 5, A5.1. The terminal verifies by means of Secure Messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity – AA

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/AA	The TSF shall provide an Active Authentication Mechanism according to [6] to prove the identity of the TOE.

(This SFR is defined in addition to BSI-CC-PP-0056 [15] to take the Active Authentication functionality into account.)

6.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2 [19]).

FDP_ACC.1 Subset access control

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

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2 [19]).

FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the Access Control SFP to objects based on the following:

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

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD
2. the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD
3. the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD

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 rule:

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

Note: The relative certificate holder authorization encoded in the CVC of the Inspection System is defined in [7], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Note: Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, EF.DG5 to EF.DG16 of the logical MRTD.

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2 [19]).

FDP_UCT.1 Basic data exchange confidentiality

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

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2 [19]).

FDP_UIT.1 Data exchange integrity

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the Access Control SFP 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	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred **after Chip Authentication**.

Rationale for Refinement: Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [1] and [16]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [16] (see FDP_UIT.1).

Note: FDP_UCT.1and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication to the General Inspection System. The authentication mechanism as part of Basic Access Control Mechanism and the Chip Authentication Protocol establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.1.5 Class FMT Security Management

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

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2 [19]).

FMT_SMF.1 Specification of Management Functions

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

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2 [19]).

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles:

1. Manufacturer
2. Personalization Agent
3. Country Verifier Certification Authority
4. Document Verifier
5. Domestic Extended Inspection System
6. Foreign Extended Inspection System

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

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

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

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1" as specified below (Common Criteria Part 2 [19] extended).

FMT_LIM.1 Limited capabilities

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow 1. User Data to be disclosed or manipulated 2. Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed 3. TSF data to be disclosed or manipulated 4. Software to be reconstructed 5. Substantial information about construction of TSF to be gathered which may enable other attacks

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 [19] extended).

FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their 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. Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed 3. TSF data to be disclosed or manipulated 4. Software to be reconstructed 5. Substantial information about construction of TSF to be gathered which may enable other attacks

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

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2 [19]). 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.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer

Note: The Pre-personalization Data include but are not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

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

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

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

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

Note: The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent (cf. [7], sec. 2.2.6). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

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

Note: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [7], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [7], sec. 2.2.3 and 2.2.4).

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

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

Note: The authorized roles are identified in their certificate (cf. [7], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3/EAC). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [7], annex A.3.3, for details).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent

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

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

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

Note: The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

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

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

(This SFR is defined in addition to BSI-CC-PP-0056 [15] to take the Active Authentication functionality into account.)

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

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

FMT_MTD.1/KEY_READ_AA Management of TSF data – Key Read – AA

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ_AA	The TSF shall restrict the ability to read the Active Authentication Private Key to none

(This SFR has been added to BSI-CC-PP-0056 [15] to take the Active Authentication functionality into account.)

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol and the Access Control

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.

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

6.1.6 Class FPT Protection of 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 [19] extended).

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to Personalization Agent Authentication Keys and Chip Authentication Private Keys and Manufacturer Authentication Keys and none.
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 Keys and Chip Authentication Private Keys and Manufacturer Authentication Keys and none.

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

FPT_EMSEC.1/AA TOE Emanation – AA

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1/AA	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to Active Authentication Private Keys and none.
FPT_EMSEC.1.2/AA	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Active Authentication Private Keys and none.

(This SFR has been added to BSI-CC-PP-0056 [15] to take the Active Authentication functionality into account.)

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 [19]).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur 2. failure detected by TSF according to FPT_TST.1

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2 [19]).

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up 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.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2 [19]).

FPT_PHP.3 Resistance to physical attack

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

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

6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

- ALC_DVS.2
- AVA_VAN.5

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

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The table 6.2 provides an overview for security functional requirements coverage.

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
FAU_SAS.1				x						
FCS_CKM.1	x	x	x		x					
FCS_CKM.4	x	x	x							
FCS_COP.1/SHA	x	x	x		x					
FCS_COP.1/SYM	x	x	x		x					
FCS_COP.1/MAC	x	x	x		x					
FCS_COP.1/SIG_VER	x		x							
FCS_COP.1/RSA_MRTD_AA										x
FCS_RND.1	x		x							
FIA_UID.1	x	x	x							
FIA_UAU.1	x	x	x							
FIA_UAU.4	x	x	x							
FIA_UAU.5	x	x	x							
FIA_UAU.6	x	x	x							
FIA_API.1					x					
FIA_API.1/AA										x
FDP_ACC.1	x	x	x							
FDP_ACF.1	x	x	x							
FDP_UCT.1			x							
FDP_UIT.1		x								
FMT_SMF.1	x	x								
FMT_SMR.1	x	x								
FMT_LIM.1						x				
FMT_LIM.2						x				
FMT_MTD.1/INI_ENA				x						
FMT_MTD.1/INI_DIS				x						
FMT_MTD.1/CVCA_INI			x							
FMT_MTD.1/CVCA_UPD			x							
FMT_MTD.1/DATE			x							
FMT_MTD.1/KEY_WRITE	x									
FMT_MTD.1/CAPK		x	x		x					
FMT_MTD.1/AAPK										x
FMT_MTD.1/KEY_READ	x	x	x		x					
FMT_MTD.1/KEY_READ_AA	x									x
FMT_MTD.3			x							
FPT_EMSEC.1	x						x			
FPT_EMSEC.1/AA	x						x			
FPT_FLS.1						x			x	
FPT_TST.1						x			x	
FPT_PHP.3							x	x		

Table 6.2: Coverage of Security Objectives for the TOE by SFR

OT.AC_Pers The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD"addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. If the Personalization Terminal want to authenticate itself 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 (for the generation of the challenge), FCS_CKM.1, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode Secure Messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6 (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/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.

OT.Data_Int The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

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

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

OT.Sens_Data_Conf 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.

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

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

The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification.

OT.Chip_Auth_Proof The security objective **OT.Chip_Auth_Proof** "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1 is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [7] requires additional TSF according to FCS_ COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode Secure Messaging).

OT.Prot_Abuse-Func

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

OT.Prot_Inf_Leak

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

OT.Prot_Phys-Tamper

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

OT.Prot_Malfunction

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

OT.Active_Auth_Proof 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_AA. The Active Authentication Protocol [6] requires additional TSF according to FCS_COP.1/RSA_MRTD_AA.

6.3.2 Dependency Rationale

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

Table 6.3 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptogr. key distribution or FCS_COP.1 Cryptogr. operation],	Fulfilled by FCS_COP.1/SYM, and FCS_COP.1/MAC,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation]	Fulfilled by FCS_CKM.1
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1/[BAC,EAC] Cryptogr. key generation],	justification 1 for non-satisfied dependencies
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/SYM	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	Fulfilled by FCS_CKM.1,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	Fulfilled by FCS_CKM.1,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/ SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	Fulfilled by FCS_CKM.1,
	FCS_CKM.4 Cryptogr. key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/ RSA_MRTD_AA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	justification 2 for non-satisfied dependencies
	FCS_CKM.4 Cryptogr. key destruction	justification 2 for non-satisfied dependencies
FCS_RND.1	No dependencies	n.a.
FCS_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control,	Fulfilled by FDP_ACC.1,
	FMT_MSA.3 Static attribute initialization	justification 3 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path],	justification 4 for non-satisfied dependencies
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1

SFR	Dependencies	Support of the Dependencies
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path],	justification 4 for non-satisfied dependencies
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/ INI_ENA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ INI_DIS	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ CVCA_INI	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ CVCA_UPD	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ DATE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ KEY_WRITE	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ CAPK	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ AAPK	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1

SFR	Dependencies	Support of the Dependencies
FMT_MTD.1/ KEY_READ	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.1/ KEY_READ_AA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMSEC.1	No dependencies	n.a.
FPT_EMSEC.1/ AA	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 6.3: Dependencies between the SFR for the TOE

Justification for non-satisfied dependencies between the SFR for TOE

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

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

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

No. 4 The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS respectively GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

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

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: Basic design

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together 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 in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance in section 6.3.3 Security Assurance Requirements Rationale 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 in sections 6.3.2 Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

Chapter 7

TOE Summary Specification (ASE_TSS.1)

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

7.1 TOE Security Functions

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

7.1.1 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. The Security Target of the hardware [3] defines the following TSFs:

TSF_INIT_A Hardware initialization & TOE attribute initialization

TSF_CONFIG_A TOE configuration switching and control

TSF_INT_A TOE logical integrity

TSF_TEST_A Test of the TOE

TSF_FWL_A Memory Firewall

TSF_PHT_A Physical tampering protection

TSF_ADMINIS_A Security violation administrator

TSF_OBS_A Unobservability

TSF_SKCS_A Symmetric Key Cryptography Support

TSF_AKCS_A Asymmetric Key Cryptography Support

TSF_ALEAS_A Unpredictable Number Generation Support

7.1.2 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/Pre-personalization – enforces Initialization and Pre-personalization policy: Configuration and initialization of the TOE, configuring of Access Control policy and doing key management only by the manufacturer (Initialization/Pre-personalization Agent) or on behalf of him (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 [7]: 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 [1, 6] 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. The delay amounts to 0.1 s, 3 s, 6 s and 10 s after the first, second, third and any further failed authentication.
  - 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

  For the BAC method, only an Enhanced-Basic Attack Potential is taken into account (see also the Note in section 6.2).
- 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 command that is not protected correctly with the session keys these are overwritten according to FIPS 140-2 [28] (or better) and a new BAC authentication is required
  - Keys in transient memory are overwritten after usage
- Active Authentication with following properties
  - According to TrPKI [6] using RSA from F.IC_CL
- Chip Authentication with following properties
  - According to TR-03110 [7] 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 [7] 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. In any case 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 [5]
- 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 [29]

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

F.Verification

TOE internal functions ensures correct operation.

7.2 Assurance Measures

The assurance measures fulfilling the requirements of EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 are given in table 7.2.

ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification 4
ADV_IMP.1	Implementation representation of the TSF 4
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
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.2	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 7.1: Assurance Measures

7.2.1 TOE Summary Specification Rationale

Table 7.2 shows the coverage of the SFRs by TSFs.

SFR	TSFs
FAU_SAS.1	F.IC_CL
FCS_CKM.1	F.IC_CL
FCS_CKM.4	F.Identification_Authentication
FCS_COP.1/SHA	F.Crypto
FCS_COP.1/SYM	F.IC_CL, F.Crypto
FCS_COP.1/MAC	F.IC_CL, F.Crypto
FCS_COP.1/SIG_VER	F.IC_CL
FCS_COP.1/RSA_MRTD_AA	F.IC_CL
FCS_RND.1	F.IC_CL
FIA_UID.1	F.Access_Control
FIA_UAU.1	F.Access_Control
FIA_UAU.4	F.Identification_Authentication
FIA_UAU.5	F.Access_Control, F.Identification_Authentication
FIA_UAU.6	F.Identification_Authentication
FIA_API.1	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	F.Identification_Authentication
FDP_UIT.1	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

SFR	TSFs
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.1/KEY_READ_AA	F.Access_Control
FMT_MTD.3	F.Identification_Authentication
FPT_EMSEC.1	F.IC_CL
FPT_EMSEC.1/AA	F.IC_CL
FPT_FLS.1	F.IC_CL
FPT_TST.1	F.IC_CL, F.Verification
FPT_PHP.3	F.IC_CL

Table 7.2: 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, TSF_INT_A, TSF_TEST_A**.

The SFR **FCS_CKM.1** requires the ECDH algorithm. This is provided by the crypto library function **F.IC_CL, TSF _AKCS_A**.

The SFR **FCS_CKM.4** 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** requires SHA-1, SHA-224 and SHA-256. **F.Crypto** provides these hash algorithms.

The SFR **FCS_COP.1/SYM** 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, TSF_SKCS_A** (Triple-DES) and **F.Crypto** (provides DES/Retail MAC).

The SFR **FCS_COP.1/MAC** 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, TSF_SKCS_A** (Triple-DES) and **F.Crypto** (provides DES/Retail MAC).

The SFR **FCS_COP.1/SIG_VER** requires ECDSA and cryptographic key sizes 224, 256 and 320 bits to perform digital Signature Verification. **F.IC_CL, TSF_AKCS_A** provides functions to verify signatures based on ECC.

The SFR **FCS_COP.1/RSA_MRTD_AA** requires RSA. **F.IC_CL, TSF_AKCS_A** provides functions.

The SFR **FCS_RND.1** requires the generation of random numbers which is provided by **F.IC_CL, TSF_ALEAS_A**. 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** 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** requires Terminal Authentication protocol, Secure Messaging in MAC-ENC mode and symmetric authentication mechanism based on Triple-DES. In addition SFR **FIA_UAU.5** 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** requires re-authentication for each command after successful authentication. This is done by **F.Identification_Authentication** providing Secure Messaging.

The SFR **FIA_API.1** 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** 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** 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 Manufacturer (Initialization/Pre-personalization Agent) performs the Initialization and configures the file layout in phase 2, 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, TSF_CONFIG_A, TSF_TEST_A** 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, TSF_CONFIG_A, TSF_TEST_A** 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, TSF_FWL_A** 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 Chip 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.1/KEY_READ_AA** requires the Active Authentication Private Key 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, TSF_OBS_A, TSF_ADMINIS_A**.

The SFR **FPT_EMSEC.1/AA** requires limiting of emanations. This is provided by **F.IC_CL, TSF_OBS_A, TSF_ADMINIS_A**.

The SFR **FPT_FLS.1** requires failure detection and preservation of a secure state. The Control of Operating Conditions of **F.IC_CL, TSF_INIT_A, TSF_INT_A, TSF_FWL_A, TSF_PHT_A, TSF_ADMINIS_A** 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** does this testing. **F.IC_CL, TSF_INT_A, TSF_TEST_A** controls all EEPROM and ROM content for integrity.

The SFR **FPT_PHP.3** requires resistance to physical manipulation and probing. This is provided by **F.IC_CL, TSF_INIT_A, TSF_PHT_A** which is provided by the hardware to resist attacks.

7.3 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the ST Microelectronics Chip SB23YR80B [3].

7.3.1 Relevance of Hardware TSFs

Table 7.3 shows the relevance of the hardware security functions for the composite Security Target.

Hardware TSFs	**Relevant**	**Not relevant**
TSF_INIT_A: Hardware init. & TOE attribute init.	x	
TSF_CONFIG_A: TOE configuration switching and control	x	
TSF_INT_A: TOE logical integrity	x	
TSF_TEST_A: Test of the TOE	x	
TSF_FWL_A: Memory Firewall	x	
TSF_PHT_A: Physical tampering protection	x	
TSF_ADMINIS_A: Security violation administrator	x	
TSF_OBS_A: Unobservability	x	
TSF_SKCS_A: Symmetric Key Cryptography Support	x	
TSF_AKCS_A: Asymmetric Key Cryptography Support	x	
TSF_ALEAS_A: Unpredictable Number Generation Support	x	

Table 7.3: Relevance of Hardware TSFs for Composite ST

7.3.2 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.MRTD_Manufact (MRTD manufacturing): No conflict
  - A.MRTD_Delivery (MRTD delivery): No conflict
  - A.Pers_Agent (Personalization of the MRTD's chip): No conflict
  - A.Insp_Sys (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
  - BSI.A.Process-Sec-IC (Protection during Packaging, Finishing and Personalization): No conflict
  - BSI.A.Plat-Appl (Usage of Hardware Platform): See BSI.OE.Plat-Appl; the correct usage of the hardware platform becomes a Security Objective of the TOE and is proven by the evaluation
  - BSI.A.Resp-Appl (Treatment of User Data): Covered by Security Objective OT.Prot_Inf_Leak

Threats

The Threats of the TOE and the hardware can be mapped (see Table 7.4) or are not relevant. They show no conflicts between each other.

- Threats of the TOE
  - 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
  - BSI.T.Leak-Inherent (Inherent Information Leakage): Matches T.Information_Leakage of the TOE ST
  - BSI.T.Phys-Probing (Physical Probing): Matches T.Phys-Tamper of the TOE ST
  - BSI.T.Malfunction (Malfunction due to Environmental Stress): Matches T.Malfunction of the TOE ST
  - BSI.T.Phys-Manipulation (Physical Manipulation): Matches T.Phys-Tamper of the TOE ST
  - BSI.T.Leak-Forced (Forced Information Leakage): Matches T.Information_Leakage of the TOE ST

- BSI.T.Abuse-Func (Abuse of Functionality): Matches T.Abuse-Func of the TOE ST
- BSI.T.RND (Deficiency of Random Numbers): Basic threat concerning especially the BAC functionality of the TOE; no conflict
- AUG4.T.Mem-Access (Memory Access Violation): Matches T.Malfunction, T.Abuse-Func and T.Phys-Tamper of the TOE

	T.Abuse-Func	T.Information_Leakage	T.Phys-Tamper	T.Malfunction
BSI.T.Leak-Inherent		x		
BSI.T.Phys-Probing			x	
BSI.T.Malfunction				x
BSI.T.Phys-Manipulation			x	
BSI.T.Leak-Forced		x		
BSI.T.Abuse-Func	x			
AUG4.T.Mem-Access	x		x	x

Table 7.4: Mapping of hardware to TOE Threats (only threats that can be mapped directly are shown)

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.BAC-PP (Fulfillment of the Basic Access Control Protection Profile): Not applicable
  - P.Sensitive_Data (Privacy of sensitive biometric reference data): Not applicable
  - 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

- Organizational Security Policies of the hardware
  - BSI.P.Process-TOE (Protection during TOE Development and Production): Covered by P.Manufact of the TOE ST
  - AUG1.P.Add Functions (Additional Specific Security Functionality): Covered by the BAC-Security Policies of the TOE

Security Objectives

Some of the Security Objectives of the TOE and the hardware can be mapped directly (see Table 7.5). None of them show any conflicts 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.Sens_Data_Conf (Confidentiality of sensitive biometric reference data): Matches AUG1.O.Add-Functions of the hardware ST
  - OT.Identification (Identification and Authentication of the TOE - BAC): Matches BSI.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 BSI.O.Abuse-Func of the hardware ST
  - OT.Prot_Inf_Leak (Protection against Information Leakage): Matches BSI.O.Leak-Inherent and BSI.O.Leak-Forced of the hardware ST
  - OT.Prot_Phys-Tamper (Protection against Physical Tampering – BAC): Matches BSI.O.Phys-Probing and BSI.O.Phys-Manipulation of the hardware ST
  - OT.Prot_Malfunction (Protection against Malfunctions): Matches BSI.O.Malfunction of the hardware ST
  - OT.Active_Auth_Proof (Proof of MRTD's chip authenticity): Matches AUG1.O.Add-Functions of the hardware ST
- Security Objectives for the hardware
  - BSI.O.Leak-Inherent (Protection against Inherent Information Leakage): Covered by OT.Prot_Inf_Leak of the TOE ST
  - BSI.O.Phys-Probing (Protection against Physical Probing): Covered by OT.Prot_Phys-Tamper of the TOE ST
  - BSI.O.Malfunction (Protection against Malfunctions): Covered by OT.Prot_Malfunction of the TOE ST
  - BSI.O.Phys-Manipulation (Protection against Physical Manipulation): Covered by OT.Prot_Phys-Tamper of the TOE ST

- BSI.O.Leak-Forced (Protection against Forced Information Leakage): Covered by OT.Prot_Inf_Leak of the TOE ST
- BSI.O.Abuse-Func (Protection against Abuse of Functionality): Covered by OT.Prot_Abuse-Func of the TOE ST
- BSI.O.Identification (TOE Identification): Covered by OT.Identification of the TOE ST
- BSI.O.RND (Random Numbers): Basic objective for the security of the TOE; no conflicts with any Security Objective of the TOE
- AUG1.O.Add-Functions (Additional specific security functionality): Covered by OT.Sens_Data_Conf and OT.Active_Auth_Proof of the TOE ST
- AUG4.O.Mem-Access (Dynamic Area based Memory Access Control): Covered by OT.Prot_Malfunction, OT.Prot_Abuse-Func and OT.Prot_Phys-Tamper of the TOE ST
- BSI.OE.Plat-Appl (Usage of Hardware Platform): The correct usage of the hardware platform becomes a Security Objective of the TOE and is proven by the evaluation
- BSI.OE.Resp-Appl (Treatment of User Data): No conflicts
- BSI.OE.Process-Sec-IC (Protection during Packaging, Finishing and Personalization): No conflicts

	OT.Sens_Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
BSI.O.Leak-Inherent				x			
BSI.O.Phys-Probing					x		
BSI.O.Malfunction						x	
BSI.O.Phys-Manipulation					x		
BSI.O.Leak-Forced				x			
BSI.O.Abuse-Func			x				
BSI.O.Identification		x					
AUG1.O.Add-Functions	x						x
AUG4.O.Mem-Access			x		x	x	

Table 7.5: Mapping of hardware to TOE Security Objectives including those of the environment (only those that can be mapped directly are shown)

Security Requirements

The relevant Security Requirements of the TOE and the hardware can be mapped directly (see Table 7.6). None of them show any conflicts 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 (Cryptographic key generation - Generation of Diffie-Hellman Keys by the TOE): Matches FCS_COP.1/Elliptic Curve cryptography operation of the hardware ST
  - FCS_CKM.4 (Cryptographic key destruction): No conflicts
  - FCS_COP.1/SHA (Cryptographic operation - Hash for Key Derivation by MRTD): Matches FCS_COP.1/SHA-[1, 224, 256] operation of the hardware ST
  - FCS_COP.1/SYM (Cryptographic operation - Symmetric Encryption / Decryption): Matches FCS_COP.1/Elliptic Curve cryptography operation of the hardware ST
  - FCS_COP.1/MAC (Cryptographic operation - Retail MAC): Matches FCS_COP.1/DES/ 3DES operation of the hardware ST
  - FCS_COP.1/SIG_VER (Cryptographic operation - Signature verification by MRTD): Matches FCS_COP.1/Elliptic Curve cryptography operation of the hardware ST
  - FCS_COP.1/RSA_MRTD_AA (Cryptographic operation - Signature creation by MRTD): Matches FCS_COP.1/RSA operation of the hardware ST
  - FCS_RND.1 (Quality metric for random numbers): Matches FCS_RNG.1 of the hardware ST
  - Class FIA (Identification and Authentication): No conflicts
  - FDP_ACC.1 (User Data Protection - Subset access control): Matches FDP_ACC.2 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): No conflicts
  - FMT_SMR.1 (Security roles): No conflicts
  - 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
  - Other Class FMT (Management of TSF data): No conflicts
  - FPT_EMSEC.1 (TOE Emanation): Matches FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 of the hardware ST
  - FPT_EMSEC.1/AA (TOE Emanation): Matches FDP_ITT.1, FPT_ITT.1 and FDP_IFC.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 of the hardware ST
  - FPT_PHP.3 (Resistance to physical attack): Matches FRU_FLT.2 and FPT_PHP.3 of the hardware ST

- Security Requirements of the hardware
  - FAU_SAS.1 (Audit storage) Matches FAU_SAS.1 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
  - FPT_FLS.1 (Failure with preservation of secure state): Covered by FPT_FLS.1 and FPT_PHP.3 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
  - FPT_PHP.3 (Resistance to physical attack): Covered by FPT_PHP.3 of the TOE ST
  - FDP_ITT.1 (Basic internal transfer protection): Covered by FPT_EMSEC.1 and FPT_EMSEC.1/AA of the TOE ST
  - FPT_ITT.1 (Basic internal TSF data transfer protection): Covered by FPT_EMSEC.1 and FPT_EMSEC.1/AA of the TOE ST
  - FDP_IFC.1 (Subset information flow control): Covered by FPT_EMSEC.1 of the TOE ST
  - FCS_RNG.1 (Random number generation): Covered by FCS_RND.1 of the TOE ST
  - FDP_ACC.2 (Complete access control) Covered by FDP_ACC.1 of the TOE ST
  - FDP_ACF.1 (Security attribute based access control) Covered by FDP_ACF.1 of the TOE ST
  - FMT_MSA.3 (Static attribute initialization): Used implicitly, no conflicts to the TOE SFRs
  - FMT_MSA.1 (Management of security attributes): Used implicitly, no conflicts to the TOE SFRs
  - FCS_COP.1 (Cryptographic operation): Covered by FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC and FCS_COP.1/SIG_VER and FCS_COP.1/RSA_MRTD_AA of the TOE ST
  - FCS_CKM.1 (Cryptographic key generation): No conflicts

	FAU_SAS.1	FCS_CKM.1	FCS_COP.1/SHA	FCS_COP.1/SYM	FCS_COP.1/MAC	FCS_COP.1/SIG_VER	FCS_COP.1/RSA_MRTD_AA	FCS_RND.1	FDP_ACC.1	FDP_ACF.1	FMT_LIM.1	FMT_LIM.2	FPT_EMSEC.1	FPT_EMSEC.1/AA	FPT_FLS.1	FPT_TST.1	FPT_PHP.3
FAU_SAS.1	x																
FRU_FLT.2															x	x	x
FPT_FLS.1															x		x
FMT_LIM.1											x						
FMT_LIM.2												x					
FPT_PHP.3																	x
FDP_ITT.1													x	x			
FPT_ITT.1													x	x			
FDP_IFC.1													x	x			
FCS_RNG.1								x									
FDP_ACC.2									x								
FDP_ACF.1										x							
FCS_COP.1		x	x	x	x	x	x										

Table 7.6: Mapping of of hardware to TOE Security SFRs (only SFRs that can be mapped directly are shown)

Assurance Requirements

The level of assurance of the

- TOE is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
- Hardware is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

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

7.3.3 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 [6] 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 / 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 [32], 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 [6] 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. [1]

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. [1]

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 [6], 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 [6]. 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). [6]

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. [33]

Extended Access Control Security mechanism identified in [6] 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. [1]

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. [33]

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. [1]

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. [33]

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. [33]

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

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

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

Issuing Organization Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [5]

Issuing State The Country issuing the MRTD. [5]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [5]. The capacity expansion technology used is the MRTD's chip.

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

1. personal data of the MRTD holder
2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1)
3. the digitized portraits (EF.DG2)
4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
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. [5]

Machine readable visa (MRV) A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [5]

Machine readable zone (MRZ) Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [5]

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [1]

MRTD application Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes

- the file structure implementing the LDS [5]
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 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 [14] and programmed according to the Logical Data Structure as specified by ICAO, [34] 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. [1]

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. [5]

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

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [1]

Secure messaging in encrypted mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [35].

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. [33]

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 [32]).

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 [32]).

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. [33]

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] ICAO. Machine Readable Travel Documents, Part 1 - Machine Readable Passports. International Civil Aviation Organization, 2006.

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

[3] STMicroelectronics. SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B Security Target - Public Version. SMD_Sx23YRxx_ST_09_002, Rev. 02.01. STMicroelectronics, 2009-09.

[4] BSI-PP-0035, Version 1.0, Security IC Platform Protection Profile, BSI, 2007-06-15.

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

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

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

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

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

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

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

[12] MTCOS Pro 2.1 EAC/ST23YR80 User Guidance, Version 1.3, Schürer, G., 2010-07-22.

[13] MaskTech GmbH. Security Target lite - Machine Readable Travel Document with ICAO Application and Basic Access Control, MTCOS Pro 2.1 BAC/ST23YR80, v1.3. MaskTech GmbH, 2011-02-10.

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

[15] BSI-CC-PP-0056, Version 1.10, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application, Extended Access Control', BSI, 2009-03-25.

[16] BSI-CC-PP-0055, Version 1.10, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Basic Access Control, BSI, 2009-03-25.

[17] SmarTrac Technology Ltd. Site Security Target for SMT1. BSI-DSZ-CC-S-0002-2009, Rev. 1.51 lite. SmarTrac Technology Ltd., 2009-09-30.

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

[19] CCMB-2009-07-002, Version 3.1, Revision 3, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Common Criteria Maintenance Board, 2009-07.

[20] CCMB-2009-07-003, Version 3.1, Revision 3, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Common Criteria Maintenance Board, 2009-07.

[21] CCMB-2009-07-004, Version 3.1, Revision 3, Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, 2009-07.

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

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

[24] TR-03111, Elliptic Curve Cryptography Based on ISO 15946, Version 1.00, BSI, 2007.

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

[26] FIPS PUB 186-3, DIGITAL SIGNATURE STANDARD (DSS), NIST, 2009-06.

[27] ECC Brainpool Standard Curves and Curve Generation, Version 1.0, Brainpool, 2005.

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

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

[30] 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.

[31] AIS 31, Version 1.0, Anwendungshinweise und Interpretationen zum Schema (AIS), BSI, 2001-09-25.

[32] 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.

[33] 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.

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

[35] 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.