NXP Java OS1 ChipDoc v1
ICAO EAC-SAC with optional AA
on P60D080JVC

-

Security Target Lite

Version 1.3

November 06, 2015

Athena Smartcard Inc., 16615 Lark Ave, Suite 202, Los Gatos CA 95032

Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Identification

ST title	**NXP Java OS1 ChipDoc v1 ICAO EAC-SAC with optional AA on P60D080JVC - Athena IDProtect Duo v12 Java Platform and Athena IASECCv2 applet on NXP P60D080JVC Dual Interface Microcontroller**
Authors	Athena Smartcard, Inc.
ST Lite reference	STLITE-IDPD12-ICAO-02
ST Lite Version Number	1.3
Date of production	06 November 2015
TOE Reference	ROM Mask Reference: OS755_ePassport_P60D080_002 IASECC Applet Athena Smartcard Solutions, Inc. **"ChipDoc v1"** Version 0105 Build 0219 Code reference: "v0105 b0219" IDProtect Athena SCS **"NXP JAVA OS1"** Release Date 0x4258 Release Level 0xFF02 Code reference: OS755_ePassport_P60D080_002 P60D080JVC NXP Revision C Identification Number P60D080PX36/9C44230 Certificate BSI-DSZ-CC-0897-V2-2014 Interfaces Contact only (J2K080) & Dual interface (J3K080) Crypto Library NXP Version 1.0 Certificate NSCIB-CC-12-36243-CR2
Common Criteria	CC version 3.1 Part 1: CCMB 2012-09-001 revision 4 [1] Part 2: CCMB 2012-09-002 revision 4 [2] Part 3: CCMB 2012-09-003 revision 4 [3]
PP Claim	Protection Profile [5-1] - Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) Version 1.3.0 Assurance level CC 3.1 (Revision 3) EAL 4 augmented Prepared By BSI, Germany Identification BSI-CC-PP-0056-V2-2012

	Protection Profile [5-2] - Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) Version 1.0 Assurance level CC 3.1 (Revision 3) EAL 4 augmented Prepared By BSI, Germany Identification BSI-CC-PP-0068-V2-2012

1.2. Composite TOE

In this Security Target, the name of the composite TOE developer (Athena Smartcard Solutions, Inc.) will be referenced as 'Athena'.

Operating System: Athena IDProtect Duo v12 (NXP JAVA OS1)

Java Card Applet: IASECCv2 (ChipDoc v1)

IDProtect with associated IASECCv2 applet are embedded on NXP P60D080JVC IC.

The composition analysis conducted in this section will use the words Platform to designate the NXP P60D080JVC IC [6, 7], Application to designate the two software components Athena IDProtect/OS755 (NXP OS1) and Athena IASECCv2 Applet (NXP ChipDoc v1), and Composite Product to designate the TOE.

According to the Composite product documentation [14], the different roles considered in the composition activities are associated as follows:

Platform Developer	NXP
Platform Evaluator	TUV-IT
Platform Certification Body	BSI
Application Developer	Athena
Composite Product Integrator	NXP
Composite Product Evaluator	Serma Technologies
Composite Product Certification Body	ANSSI
Composite Product evaluation Sponsor	Athena

The platform was evaluated to CC EAL 5+ according to BSI-PP-0035-2007 [8] (see platform Security Target [10], IC certification report [9]).

Integration of the composite product by the IC manufacturer is guided by delivery procedures enforced by Athena and NXP.

1.3. TOE Overview

The protection profiles [5-1] and [5-2] define 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). This ST extends this PP to contact, contactless and dual interface smartcard modules. It addresses the advanced security methods Basic Access Control (BAC), Standard Inspection Procedure (PACE), Extended Access Control (EAC) and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [15] and [16-1] for SAC (also known as PACE mechanism defined in [5-2]).

Athena IDProtect Duo v12 passport application is configurable in BAC or EAC chip authentication modes, with or without Active Authentication [15]. Also, it supports contact and contactless communication.

This ST applies to the EAC configuration with or without Active Authentication.

Note that there is no non-TOE hardware/software/firmware that is required by the TOE.

1.3.1. TOE Definition

The Target of Evaluation (TOE) is the integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [15] and providing the EAC and SAC mechanism according to the 'ICAO Doc 9303' [15] and BSI TR-03110 [16], respectively.

The TOE comprises at least:

- the circuitry of the MRTD's chip (P60D080JVC IC [6])
- the IC Embedded Software (OS1 Operating System)
- the MRTD application (ChipDoc v1 applet in ICAO configuration)
- the associated guidance documentation

1.3.2. TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this TOE 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 (such as CAN for PACE authentication) according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional 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.

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) [15]. 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 (BAC and/or SAC to the logical MRTD, Active Authentication of the MRTD's chip, EAC to the logical MRTD and the Data Encryption of additional sensitive biometrics) as optional security measure in the 'ICAO Doc 9303' [15]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This TOE 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 EAC Mechanism. This TOE addresses the AA as an optional security mechanism.

1.4. TOE Description

1.4.1. General

The TOE is an MRTD IC where application software is masked in ROM and that can be assembled in a variety of form factors. The main form factor is the electronic passport, a paper book passport embedding a contactless module:

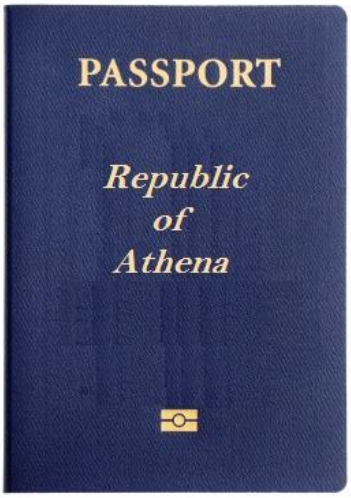


Figure 1 – TOE Main Form Factor *(photo non-contractual)*

The followings are an informal and non-exhaustive list of example graphic representations of possible end products embedding the TOE:

- Contactless interface cards and modules
- Dual interface cards and modules
- Contact only cards and modules
- SOIC8 package
- QFN44 package
- Chip on Board (PCB)

The scope of this TOE is covered in section 1.3.1 above.

The TOE is linked to a MRTD reader via its HW and physical interfaces.

- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The optional contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.
- The optional interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The optional interfaces of the TOE QNF-44 are JEDEC compliant.

There are no other external interfaces of the TOE except the ones described above.

The antenna and the packaging, including their external interfaces, are out of the scope of this TOE.

The TOE may be applied to a contact reader or to a contactless reader, depending on the external interface type(s) available in its form factor. The readers are connected to a computer and allow application programs (APs) to use the TOE.

1.4.2. MRTD's chip

For this TOE the MRTD is viewed as unit of

(1) 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

   a. the biographical data on the biographical data page of the passport book,
   b. the printed data in the Machine Readable Zone (MRZ) and
   c. the printed portrait.

(2) The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [15] 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

   a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   b. the digitized portraits (EF.DG2),
   c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
   d. the other data according to LDS (EF.DG5 to EF.DG16) and
   e. the Document security object.

This TOE addresses the protection of the logical MRTD:

- in integrity by write-only-once access control and by physical means, and
- in confidentiality by the SAC and Extended Access Control Mechanism.

This TOE addresses the Chip Authentication described in [16-1] as an alternative to the Active Authentication stated in [15].

1.4.3. Basic Access Control

The confidentiality by Basic Access Control (BAC) is a mandatory security feature that is implemented by the TOE. For BAC, the inspection system

(i) reads optically the MRTD,
(ii) authenticates itself as an 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 [15], normative appendix 5.

In compliance with the ICAO Extended protection profile [5-1], this ST requires the TOE to implement the Chip Authentication defined in [16-1]. The Chip Authentication prevents data traces described in [15], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps:

(i) the inspection system communicates by means of secure messaging established by Basic Access Control,
(ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,
(iii) the inspection system generates an ephemeral key pair,
(iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and
(v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

1.4.4. PACE

The confidentiality by Password Authenticated Access Control (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the “Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)” [R7]. Note that [R7] considers high attack potential.

For the PACE protocol according to [R17], the following steps shall be performed:

(i) The travel document’s chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

(iii) The travel document’s chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

1.4.5. Extended Access Control

In compliance with the ICAO Extended protection profile [5-1], this ST requires the TOE to implement the Extended Access Control as defined in [16-1]. 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 Certificate

1.4.6. Active Authentication

This TOE offers an optional mechanism called Active Authentication and specified in [16-1] section 1.2. This security feature is a digital security feature that prevents cloning by introducing a chip-individual key pair:

(i) The public key is stored in data group DG15 and thus protected by Passive Authentication.

(ii) The corresponding private key is stored in secure memory and may only be used internally by the MRTD chip and cannot be read out.

Thus, the chip can prove knowledge of this private key in a challenge-response protocol, which is called

Active Authentication. In this protocol the MRTD chip digitally signs a challenge randomly chosen by the inspection system. The inspection system recognizes that the MRTD chip is genuine if and only if the returned signature is correct. Active Authentication is a straightforward protocol and prevents cloning very effectively, but introduces a privacy threat: Challenge Semantics (see Appendix F for a discussion on Challenge Semantics).

1.5. TOE Limits

The TOE boundaries are the following:

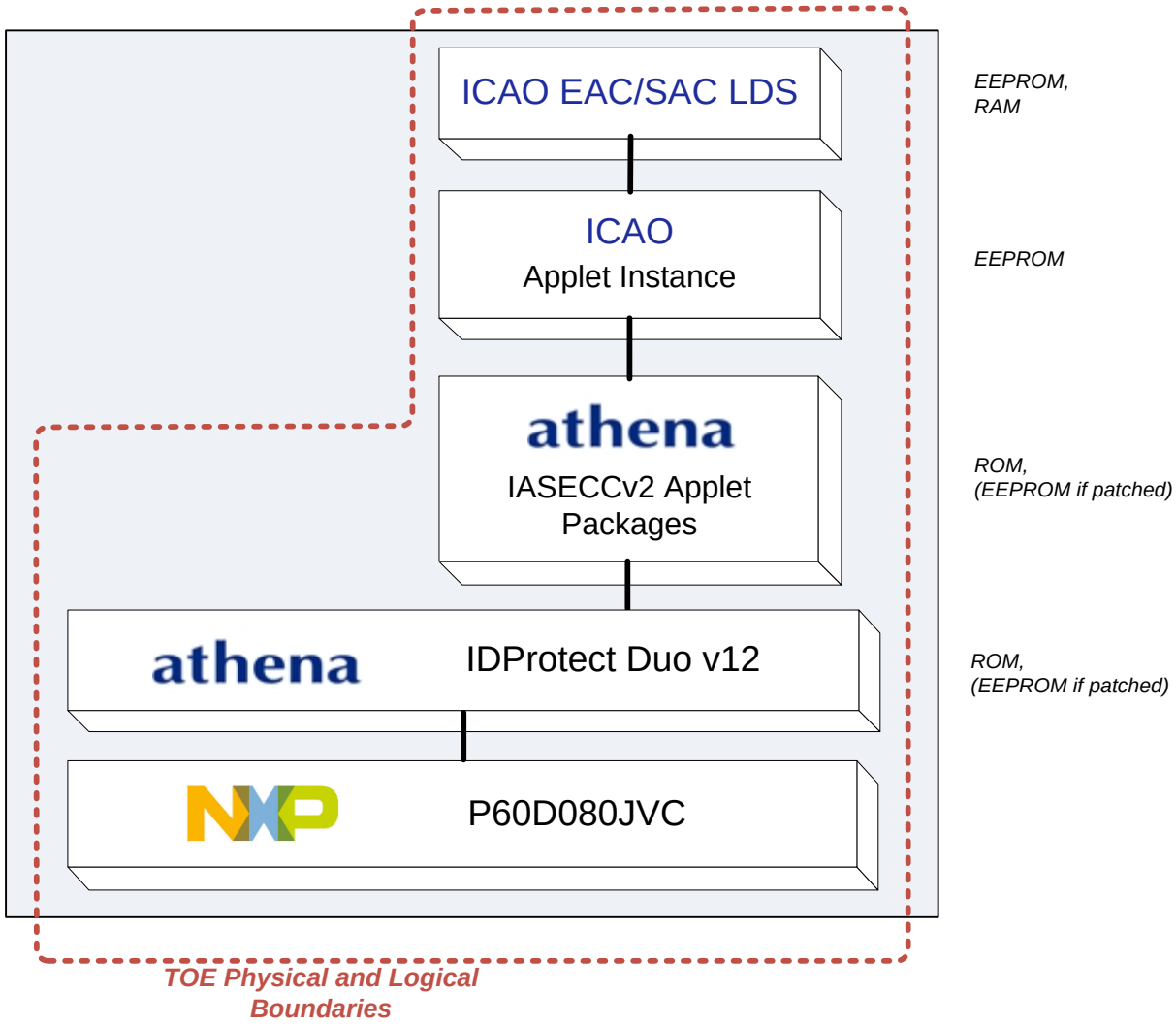


Figure 2 – TOE Description

Only IASECCv2 applet packages are present in ROM and EEPROM. The IASECCv2 Applet instance could be configured into ICAO or IAS-ECC. Only the ICAO applet instance configuration is part of the TOE. No other applet instance is present on this TOE.

In a general aspect, IDProtect Operating System enforces separation of the data between the applets and associated packages imposing logical separation of data using the Java Card™ Firewall [11-JCRE]. Athena IDProtect duo v12 is a GlobalPlatform 2.2.1 and Java Card 3.0.4 compliant Operating System that provides applets with standard services as defined in the related GlobalPlatform [13] and Java Card specifications [12].

The portions of the Applet Packages and Operating System present in EEPROM are the patches.

The hardware platform on which the Operating System is implemented is the NXP P60D080JVC IC. This IC is certified according to CC EAL 6+ [9] with the Security Target compliant with BSI-PP-0035-2007 [8].

1.6. TOE Guidance

The TOE guidance comprises the following documentation:

Title	Date	Version
ChipDoc v1 ICAO EAC Operation Manual	*Consult certification report for applicable dates and versions*	
ChipDoc v1 ICAO EAC Preparation Manual		

1.7. TOE lifecycle

The TOE lifecycle is shown in Figure 3.

The integration phase is added to the PP generic lifecycle as this particular TOE requires that card production phase is refined.

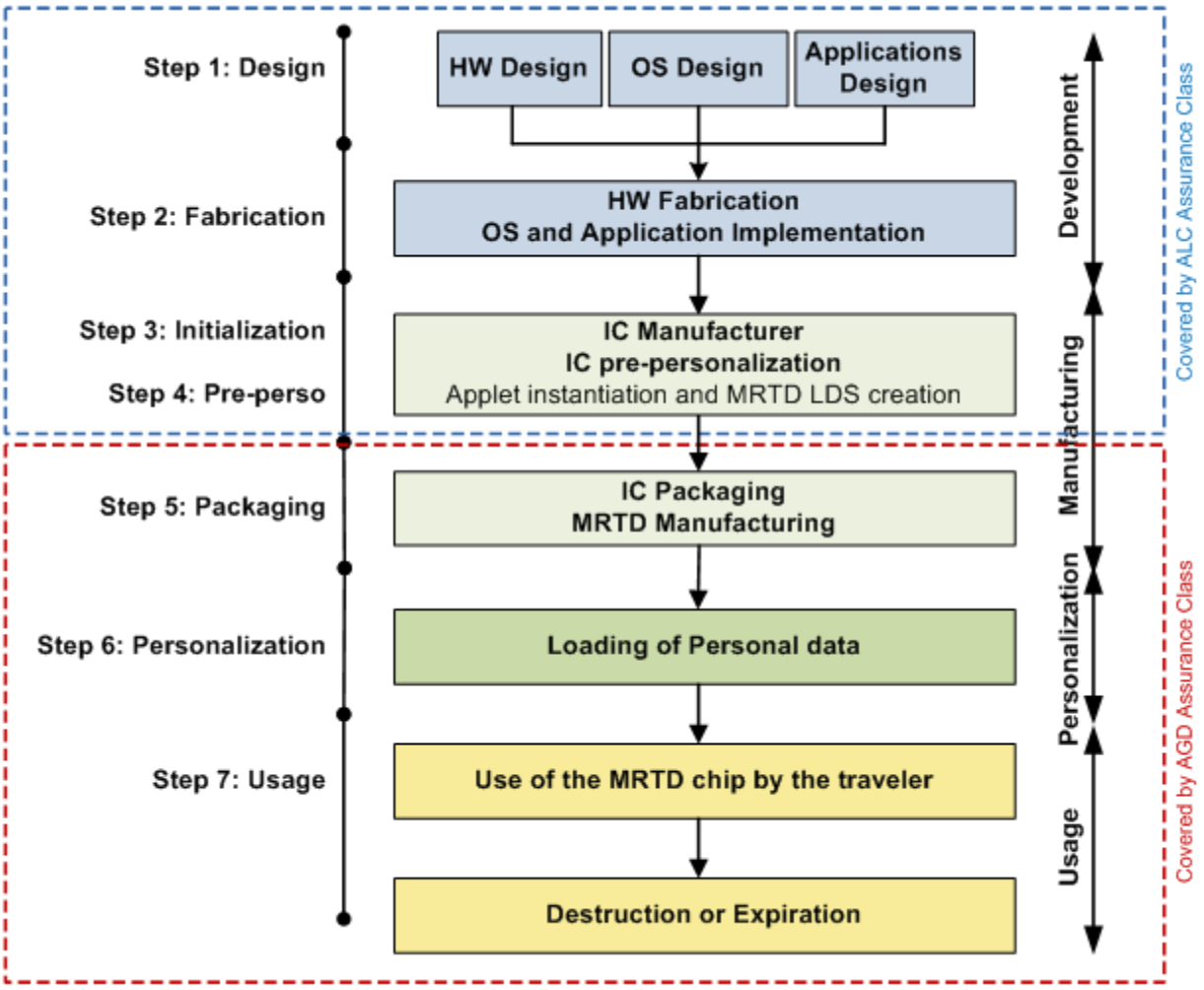


Figure 3 – TOE lifecycle

1.7.1. Phase 1 “Development”

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

HW Design – NXP

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.

OS Design – Athena Engineering departments – Livingston, Scotland
Application Design – Athena Engineering departments – Los Gatos, US

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.

1.7.2. Phase 3 “Personalization of the MRTD”

(Step 6)
The personalization of the MRTD includes:

- the survey of the MRTD holder’s biographical data,
- the enrolment of the MRTD holder biometric reference data,
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD and
- configuration of the TSF if necessary.

The step 6 is performed by the Personalization Agent and includes but is not limited to the creation of the digital MRZ data (EF.DG1), the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both, the other data according to LDS (EF.DG5 to EF.DG16) and the Document security object. The signing of the Document security object by the Document signer [15] 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.

Personalization – 3rd Party Personalization facility

The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.
The Personalization phase is not part of the scope of this TOE.

1.7.3. Phase 2 “Manufacturing”

(Step 2)
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.
HW Fabrication and OS & Application implementation – NXP

(Step 3)
The IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). Patch mechanism is terminated in this phase.

IC Manufacturing – NXP

The Operating System and applicative parts of the TOE which are developed by Athena are sent in a secure way to NXP for masking in NVM. In addition to the TOE, the mask contains confidential data, knowledge of which is required in order to initialize and personalize the chip. Additional Java Card applets developed by Athena are included in the mask and the corresponding converted files (.cap or.jca) are

also provided to NXP.

(Step 4)

During the step Pre-Perso, the MRTD manufacturer

i. creates the MRTD application and
ii. equips MRTD's chips with pre-personalization Data.

IC Pre-Personalization – NXP

Creation of the application implies applet instantiation and the creation of MF and ICAO.DF. Card Content Loading and Installing mechanism is terminated in this phase.

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

(Step 5)

The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

IC Packaging – NXP
MRTD Manufacturing – NXP

This step corresponds to the integration of the hardware and firmware components into the final product body. The TOE is protected during transfer between various parties. IC Packaging and MRTD Manufacturing are not part of the scope of this TOE.

1.7.5. Phase 4 “Operational Use”

Where upon the card is delivered to the MRTD holder and until MRTD is expired or destroyed.

(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.
The Operational Use phase is not part of the scope of this TOE.

2. Conformance Claims

2.1. CC Conformance Claim

The ST claims compliance with the following references:

- Common Criteria Version 3.1 Part 1 [1]
- Common Criteria Version 3.1 Part 2 [2] extended
- Common Criteria Version 3.1 Part 3 [3] conformant

Extensions are based on the Protection Profiles (PP [5-1] and PP [5-2]) presented in the next section:

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FIA_API.1 ‘Authentication Proof of Identity’
- FMT_LIM.1 ‘Limited capabilities’
- FMT_LIM.2 ‘Limited availability’
- FPT_EMSEC.1 ‘TOE emanation’

The assurance level for this ST is EAL 5 augmented with:

- ALC_DVS.2, and
- AVA_VAN.5

2.2. PP Claim

This ST claims strict conformance to the following Protection Profiles:

Protection Profile [5-1] **Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP)**	
Version	1.3.0
Date	20th January 2012
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0056V2
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0056-V2-2012
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Protection Profile [5-2] **Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)**	
Version	1.0
Date	2nd November 2011
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0068V2
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0068-V2-2011
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

The ICAO SAC and EAC PPs define 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 SAC and Extended Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [15] along with its supplements [16-2] and [16-3].

This MRTD's IC does not limit the TOE interfaces to contactless: both contact and contactless interfaces are part of this TOE and the PP content has been enhanced for this purpose.

3. Security Problem Definition

3.1. Assets

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

Logical MRTD sensitive User Data

Sensitive biometric reference data (Integrity and Confidentiality):

- **EF.DG3**: Biometric Finger(s)
- **EF.DG4**: Biometric Eye(s) Iris

Logical MRTD data

The 'ICAO Doc 9303' [15] requires that Basic Inspection Systems must have access to the following logical data which integrity should always be preserved (integrity, Confidentiality and Authenticity when PACE is used):

- **EF.COM**: Common Data Elements, lists the existing EF with the user data
- **EF.SOD**: Document Security Object according to LDS [15] used by the inspection system for Passive Authentication of the logical MRTD
- **EF.DG1**: document's data (Type, Issuing State or Organization, Number, Expiry Date, Optional Data), holder's data (Name, Nationality, Date of Birth, Sex) and Check Digits
- **EF.DG2**: Encoded Face (Global Interchange Feature)
- **EF.DG5**: Biometric Face
- **EF.DG7**: Displayed Signature or Usual Mark
- **EF.DG8**: Displayed Portrait
- **EF.DG9**: Data Feature(s)
- **EF.DG10**: Structure Feature(s)
- **EF.DG11**: Additional Personal Detail(s)
- **EF.DG12**: Additional Document Detail(s)
- **EF.DG13**: optional Detail(s)
- **EF.DG14**: Security Info (Chip Authentication Public Key Info)
- **EF.DG15**: Active Authentication Public Key Info
- **EF.DG16**: Person(s) to Notify

Due to interoperability reasons with 'ICAO Doc 9303' [15], the TOE specifies 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) (DG6 is absent),
- 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).

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. This authenticity relies on the confidentiality and integrity of data such as the Active Authentication Public Key, PACE key, EF.CARDACCESS info or the Chip Authentication Private Key.

3.2. Subjects

This Security Target considers the following subjects:

S.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.

S.Personalizer *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 [15].

S.Country *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.

S.DV *Document Verifier*

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

S.Terminal

A terminal is any technical system communicating with the TOE through its physical interfaces.

S.IS-PACE *Inspection system*

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 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 IS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. 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.

S.Holder *MRTD Holder*

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

S.Traveler

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

3.3. Assumptions

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

A.Insp_Sys	*Inspection Systems for global interoperability*

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE and/or BAC (with optional Active Autnehtication). BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A.Passive_Auth	*PKI for Passive Authentication*

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation 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 travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data.

A.Auth_PKI	*PKI for Inspection Systems*

The issuing and receiving States or Organisations 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 Organisations 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 Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

3.4. Threat agent

S.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. This threat agent has high attack potential.

***Application 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.*

3.5. Threats

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*

An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [8]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document'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 the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

T.Counterfeit *Counterfeit MRTD's chip*

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

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

T.Skimming *Skimming travel document / Capturing card-Terminal communication*

An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE.

T.Eavesdropping *Eavesdropping on the communication between the TOE and the PACE terminal*

An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.

T.Tracing *Counterfeit MRTD's chip*

An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

T.Forgery *Forgery of data on MRTD's chip*

An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

T.Abuse-Func *Abuse of Functionality*

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order

(i) to manipulate or to disclose the User Data stored in the TOE,
(ii) to manipulate or to disclose the TSF-data stored in the TOE or
(iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

T.Information_Leakage *Information Leakage from MRTD's chip*

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

T.Phys-Tamper *Physical Tampering*

An attacker may perform physical probing of the travel document in order

(i) to disclose the TSF-data, or
(ii) to disclose/reconstruct the TOE's Embedded Software.

An attacker may physically modify the travel document in order to alter

(I) its security functionality (hardware and software part, as well),
(II) the User Data or the TSF-data stored on the travel document.

T.Malfunction *Counterfeit MRTD's chip*

An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to

(i) deactivate or modify security features or functionality of the TOE' hardware or to
(ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

3.6. Organisational Security Policies

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

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 travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation 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 travel document'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 Version 1.

P.Manufact *Manufacturing of the MRTD's chip*

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key

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

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

This PP includes all OSPs from the PACE PP, chap 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal. Due to identical definitions and names they are also not repeated here.

P.Pre-operational *Pre-operational handling of the travel document*

1) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.

2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE27.

3.) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 above.

4.) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy..

P.Card_PKI *PKI for Passive Authentication*

1) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA) .

2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [6], 5.5.1. The CSCA shall

create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [6], 5.5.1.

3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworth_PKI *Trustworthiness of the PKI*

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

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

The Basic Inspection Systems with PACE (IS-PACE) shall operate their terminals as follows:

1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders.

2.) They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order28. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3.) The related terminals need not to use any own credentials.

4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document).

5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

4. Security Objectives

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

4.1. SOs 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.Sens_Data_Conf *Confidentiality of sensitive biometric reference data*

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical travel document 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.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 [16-1]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

Application note: *The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [15] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.*

OT.AA_Proof *Proof of MRTD's chip authenticity by Active Authentication*

The TOE may support the Extended 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 [15].

OT.Data_Int *Integrity of data*

The TOE must ensure integrity of the User Data and the TSF-data29 stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Aut *Authenticity of data*

The TOE must ensure authenticity of the User Data and the TSF-data30 stored on it by enabling verification of their authenticity at the terminal-side31.The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)

OT.Data_Conf *Confidentiality of data*

The TOE must ensure confidentiality of the User Data and the TSF-data33 by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing *Tracing travel document*

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance

OT.Prot_Abuse-Func *Protection against Abuse of Functionality*

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order

(i) to manipulate or to disclose the User Data stored in the TOE,
(ii) to manipulate or to disclose the TSF-data stored in the TOE,
(iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak *Protection against Information Leakage*

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

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

OT.Prot_Phys-Tamper *Protection against Physical Tampering*

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

OT.Prot_Malfunction	*Protection against Malfunctions*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application 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.AC_Pers	*Access Control for Personalization of logical MRTD*

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [6] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application 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) cannot be changed by write access after personalization,

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

OT.Identification	*Identification and Authentication of the TOE*

The TOE must provide means to store Initialisation and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

4.2. Objective on the Environment

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

OE. Auth_Key_Travel_Document Travel document authentication keys

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

(i) generate the travel document'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 Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE. Active_Auth_Travel_Document Travel document active authentication keys

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

(i) generate the travel document's Active Authentication Key Pair,
(ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15
(iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Active Authentication Public Key by means of the Document Security Object.

OE.Authoris_Sens_Data *Authorisation for Use of Sensitive Biometric Reference Data*

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

OE.Exam_travel_document *Examination of the physical part of the travel document*

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [4] and/or the Basic Access Control [6]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

OE.Prot_Logical_Travel_Document *Protection of data from the logical travel document*

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

OE.Ext_Insp_system *Authorization of extended inspection system*

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

OE.Legislative_Compliance *Issuing of the travel document*

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

OE.Passive_Auth_Sign *Authentication of travel document by Signature*

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must

(i) generate a cryptographically secure CSCA Key Pair
(ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and
(iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

(i) generate a cryptographically secure Document Signing Key Pair,
(ii) ensure the secrecy of the Document Signer Private Key,
(iii) hand over the Document Signer Public Key to the CSCA for certification,
(iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [6].

The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [6]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document

OE.Personalization *Personalization of logical MRTD*

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf

(i) establish the correct identity of the travel document holder and create the biographical data for the travel document,
(ii) enrol the biometric reference data of the travel document holder,
(iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder,
(iv) write the document details data,
(v) write the initial TSF data,
(vi) sign the Document Security Object (in the role of a DS).

OE.Terminal *Terminal Operating*

The terminal operators must operate their terminals as follows:

1.)The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [6].

2.)The related terminals implement the terminal parts of the PACE protocol [4], of the Passive Authentication [4] (by verification of the signature of the Document Security Object) and use them in this order37. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3.)The related terminals need not to use any own credentials.

4.)The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [6]).

5.)The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

OE.Travel_Document_Holder *Travel document holder obligations*

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

4.3. Security objectives rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

4.3.1. Security Objectives Coverage

The following able indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Threats Assumptions Policies / Security objectives	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.AA_Proof	OT.OT.AC_Pers	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Auth_Key_Travel_Document	OE.Active_Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.OE.Personalisation	OE-Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Read_Sensitive_Data	X															X			X					
T.Counterfeit		X	X											X	X		X							
T.Skimming					X	X	X																X	
T.Eavesdropping							X																	
T.Tracing								X															X	
T.Abuse-func									X															
T.Information_Leakage										X														
T.Phys-Tamper												X												
T.Malfunction													X											
T.Forgery					X	X	X		X			X					X			X	X	X		
P.Sensitive_data	X															X			X					
P.Personalization				X							X									X				
P.Manufact											X													
P.Pre-Operational				X							X									X				X
P.Terminal																	X					X		
P.Card_PKI																					X			
P.Thrustworthy_PKI																					X			
A.Insp_Sys																	X	X						
A.Auth_PKI																X			X					
A.Passive_Auth																	X				X			

Table 1 – Security Environment to Security Objectives Mapping

4.3.2. Security Objectives Sufficiency

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objectives **OT.Data_Inty**, **OT.Data_Aut** and **OT.Data_Conf** through the PACE authentication. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective **OT.Data_Conf** through a trusted channel based on the PACE authentication.

The threat **T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives **OT.Tracing** (no gathering TOE tracing data) and **OE.Travel_Document_Holder** (the attacker does not a priori know the correct values of the shared passwords).

The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective **OT.AC_Pers** requires the TOE to limit the write access for the travel document to the trustworthy Personalisation Agent (cf. **OE.Personalisation**). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives **OT.Data_Int** and **OT.Data_Aut**, respectively. The objectives **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to **OE.Terminal** and performing the Passive Authentication using the Document Security Object as aimed by **OE.Passive_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally, the examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft- coded security functionality. The security objective **OT.Prot_Abuse-Func** ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives **OT.Prot_Inf_Leak**, **OT.Prot_Phys-Tamper** and **OT.Prot_Malfunction**, respectively.

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

The OSP **P.Pre-Operational** is enforced by the following security objectives: **OT.Identification** is affine to the OSP's property 'traceability before the operational phase'; **OT.AC_Pers** and **OE.Personalisation** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents'; **OE.Legislative_Compliance** is affine to the OSP's property 'compliance with laws and regulations'.

The OSP **P.Terminal** is obviously enforced by the objective **OE.Terminal**, whereby the one-to-one mapping between the related properties is applicable. Additionally, this OSP is countered by the security objective **OE.Exam_Travel_Document**, that enforces the terminals to perform the terminal part of the PACE protocol.

The OSP **P.Card_PKI** is enforced by establishing the issuing PKI branch as aimed by the objectives **OE.Passive_Auth_Sign** (for the Document Security Object).

The OSP **P.Trustworthy_PKI** is enforced by **OE.Passive_Auth_Sign** (for CSCA, issuing PKI branch).

The Assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly addressed by **OE.Passive_Auth_Sign** requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document.

The OSP **P.Personalisation** “Personalisation of the travel document by issuing State or Organisation only” addresses the (i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** “Personalisation of logical travel document”, and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document”. Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation 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 Organisation 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 OSP P.Terminal “Abilities and trustworthiness of terminals” is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [7]. **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** “Counterfeit of travel document chip data” addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organisation. 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_Travel_Document** “Travel document Authentication Key”. According to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document’s chip.

In addition, the threat **T.Counterfeit** “Counterfeit of travel document chip data” is countered by chip an identification and authenticity proof required by **OT.Active_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organisation. The 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_Travel_Document** “Travel document Authentication Key”.

5. Extended Components Definition

This ST contains the following extended components defined as extensions to CC part 2 in the claimed Protection Profile [5-1]:

- SFR FAU_SAS ‘Audit data storage’
- SFR FCS_RND ‘Generation of random numbers’
- SFR FIA_API ‘Authentication Proof of Identity’
- SFR FMT_LIM ‘Limited capabilities and availability’
- SFR FPT_EMSEC.1 ‘TOE emanation’

5.1. Audit data storage (FAU_SAS)

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

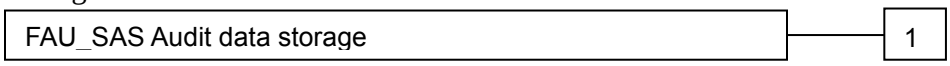
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

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

Component leveling:



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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.2. Generation of random numbers (FCS_RND)

To define the IT security functional requirements of the TOE, a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

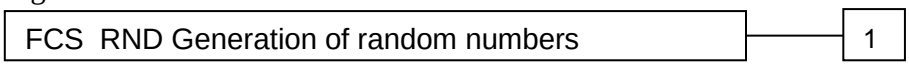
The family "Generation of random numbers (FCS_RND)" is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3. Authentication Proof of Identity (FIA_API)

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

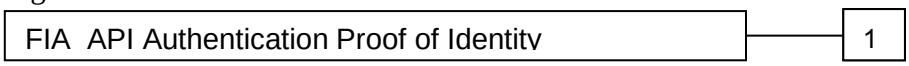
Application note: *The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Extended Components definition (ASE_ECD)") from a TOE point of view.*

FIA_API Authentication Proof of Identity

Family behavior

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

Component leveling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.4. Limited capabilities and availability (FMT_LIM)

The family FMT_LIM describes the functional requirements for the Test Features of the TOE.

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

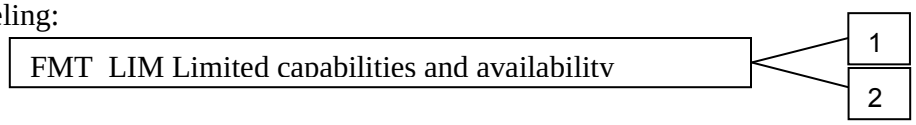
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

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

Component leveling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 **The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].**

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 **The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].**

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

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

or conversely

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

The combination of both requirements shall enforce the policy.

5.5. TOE emanation (FPT_EMSEC.1)

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

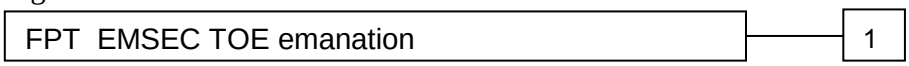
The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FPT_EMSEC TOE Emanation

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



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

6. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Some security functional requirements represent extensions to [2].

Operations for assignment, selection and refinement have been made and are designated by an underline (e.g. none), in addition, where operations that were uncompleted in the PP [5-1] are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 0 is drawn from the security assurance components from Common Criteria part 3 [3].

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 3.2. Note that all these subjects are acting for homonymous external entities. All used objects are defined either in section 9 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [2]. The operation “load” is synonymous to “import” used in [2].

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [16-1], 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. [16-1], 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. [16-1], 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. [16-1], 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. [16-1], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [16-1], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [16-1], A.5.1)

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

Name	Certificate Data
CVCA Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
CVCA Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA 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.

Name	Certificate Data
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [16-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) 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 (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) 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 (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Active Authentication Key Pair	The Active Authentication asymmetric Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication Protocol: allowing the chip to be authenticated as genuine by the inspection system.
Active Authentication Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to be authenticated as a genuine MRTD's chip by the inspection system. It is part of the TSF data.
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
PACE Session Keys (PACE-KMAC, PACE-KENC)	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol.
PACE authentication ephemeral key pair (ephem-SKPICC-PACE, ephem-PKPICC-PACE)	The ephemeral PACE Authentication Key Pair (ephem-SKPICC-PACE, ephem-PKPICC-PACE) is used fot Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03110.
Ephem-PKPICC-PAC	PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) 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.
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.

Name	Certificate Data
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 TDES 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 TDES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Application 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. TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. Audit Storage (FAU_SAS.1)

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

Application note: *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. Cryptographic support (FCS)

Function		Algorithm	Key Size(s)
Chip Authentication	Hashing	SHA-1	-
	Authentication	DH	1024, 1536, 2048 bits
		ECDH	(NIST) 192, 224, 256, 320, 384, 521 bits (Brainpool) 192, 224, 256, 320, 384, 512 bits
PACE	Authentication	DH-GM	1024, 1536, 2048 bits
		ECDH-GM	(NIST) 192, 224, 256, 320, 384, 521 bits (Brainpool) 192, 224, 256, 320, 384, 512 bits
Terminal Authentication	Signature verification	RSA Pad: PKCS#1 (v1.5 [11] or PSS [23]) Hash: SHA-1, SHA-256	1024, 1280, 1536, 2048 bits
		ECDSA Hash: SHA-1, SHA-224, SHA-256	192, 224, 256, 384, 521 bits
Active Authentication	Signature generation	RSA ISO9796-2 scheme 1	1024, 1280, 1536, 2048 bits
Secure Messaging	ENC/DEC	TDES CBC [22]	112 bits
		AES	128, 192, 256 bits
	MAC	Retail MAC	112 bits
		CMAC 8	-

6.1.2.1. Cryptographic key generation (FCS_CKM.1)

→ Chip Authenticate keys generation

FCS_CKM.1.1/ CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3 [19], or ECDH compliant to ISO 15946 [20]* and specified cryptographic key sizes *DH 1024-1536-2048 bits or ECDH NIST curves 192-224-256-320-384-521 bits or ECDH Brainpool curves 192-224-256-320-384-512 bits respectively* that meet the following: [16-1] Annex A.1.

Application note: *The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [16-1], sec. 3.1 and Annex A.1. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [19]) or on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [16-1] Annex A.1, [20] and [17] for details). The shared secret value is used to derive the* TDES *key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [15], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/ENC and FCS_COP.1/MAC.*

→ PACE keys generation

FCS_CKM.1.1/ DH_PACE — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3 [19], or ECDH compliant to ISO 15946 [20]* and specified cryptographic key sizes *DH 1024-1536-2048 bits or ECDH Generic Mapping NIST curves 192-224-256-320-384-521 bits or ECDH Generic Mapping Brainpool curves 192-224-256-320-384-512 bits respectively* that meet the following: [16-1] Annex A.1.

→ Cryptographic Key Pair generation

FCS_CKM.1.1/ KP — The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA and EC key pair generation* and specified cryptographic key sizes *RSA 1024-1280-1536-2048 bits or EC 192-224-256-384-521 bits respectively* that meet the following: *IEEE 1363 [23]*.

Application note: *The component FMT_MTD.1/PK applies to both the Active Authentication Private Key and the Chip Authentication Private Key. This component defines an operation "create" that means here that these keys are generated by the TOE itself. This resulted in this instantiation of the component FCS_CKM.1 as SFR for the generation of these two key.*

6.1.2.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 — The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *none*.

Application note: *The TOE destroys the BAC Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol. The TOE destroys the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new power-on-session.*

6.1.2.1. Cryptographic operation (FCS_COP.1)

→ Hashing

FCS_COP.1.1/ SHA — The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1, SHA-224 or SHA-256* and cryptographic key sizes none that meet the following: *FIPS 180-2 [21]*.

Application note: *The Chip Authentication Protocol uses SHA-1 (cf. [16], normative appendix 5, A5.1). The TOE implements additional hash function SHA-256 and SHA-224 for the Terminal Authentication Protocol (cf. [16], Annex A.2.2). SHA-224 is supported by the TOE for ECDSA Signature operations only.*

→ SM Encrypt/Decrypt Chip Authentication

FCS_COP.1.1/ CA_ENC — The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *TDES in CBC mode* and cryptographic key sizes *112 bits* that meet the following: *FIPS 46-3 [22] and 'TR-03110', [16-1]*.

Application note: *The TOE implements the cryptographic primitives (e.g. TDES) 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.*

→ SM – MAC Chip Authentication

FCS_COP.1.1/ CA_MAC — The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *Retail MAC (DES) and CMAC (AES)* and cryptographic key sizes *112 for retail MAC and 128, 192 and 256 bit for CMAC* that meet the following: *[16-3], FIPS PUB 46-3 Data Encryption Standard (DES) [22] and [24]*.

Application note: *The TOE implements 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/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.*

→ Signature verification

FCS_COP.1.1/ SIG_VER — The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm *RSA or ECDSA* and cryptographic key sizes *RSA 1024-1280-1536-2048 bits or ECDSA 192-224-256-384-521 bits respectively* that meet the following: *PKCS#1 v1.5 [11] or PKCS#1 PSS [23] and FIPS 180-2 [21]*.

Application note: *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.*

→ Signature generation

FCS_COP.1.1/ SIG_GEN — The TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *RSA 1024-1536-2048 bits* that meet the following: *ISO/IEC 9796-2 [18]*.

Application note: *For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).*

→ SM Encrypt/Decrypt PACE

FCS_COP.1.1/ PACE_ENC — The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *AES and TDES in CBC mode* and cryptographic key sizes *112 bits (for TDES)* and *128, 192 and 256 bits (for AES)* that meet the following: : *FIPS 46-3 [22], NIST [25], 'TR-03110', and [16-3]*.

→ SM – MAC PACE

FCS_COP.1.1/ PACE_MAC — The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *CMAC and Retail MAC* and cryptographic key sizes *112, 128, 192 and 256 bits* that meet the following*[16-3], FIPS PUB 46-3 Data Encryption Standard (DES) [22] and [24],[16-4] NIST [25] and [26].*

6.1.2.2. Random Number Generation (FCS_RND.1)

FCS_RND.1.1 — The TSF shall provide a mechanism to generate random numbers that meet *AIS31 class "P2 – SOF-High"*.

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

6.1.3. Identification and authentication (FIA)

The following table 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 Protocol	FIA_API.1
PACE protocol	FIA_UAU.1/PACE FIA_UAU.4/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE FIA_AFL.1/PACE

Note: the Chip Authentication Protocol as defined in the PP [5-1] includes:

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [15] 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. 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.

6.1.3.1. Authentication Failure Handling (FIA_AFL.1)

→ PACE

FIA_AFL.1.1/ PACE	The TSF shall detect when a **defined integer number between 1 and 255** unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.
FIA_AFL.1.2/ PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall **send the response to the authentication request with a few seconds delay**

***Application Note**: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [R16-3]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy, the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP. One of some opportunities for performing this operation might be "consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords".*

***Application Note**: The count of consecutive unsuccessful authentications is stored in non-volatile memory and is preserved across power-up and power-down cycles. After a successful authentication the count is reset to zero.*

6.1.3.2. Timing of identification (FIA_UID.1)

FIA_UID.1.1/PACE The TSF shall allow
1. to establish the communication channel,
2. carrying out the PACE Protocol according to [R16-3],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol v.1 according to [R16-1]68
5. to carry out the Terminal Authentication Protocol v.1 according to [R16-1]69
6. **to carry out the Active Authentication Mechanism**

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

FIA_UID.1.2/PACE The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application 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 may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. PP MRTD BAC [4]) is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this PP, it is a mandatory part within the Chip Authentication Protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).*

Application Note*: User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).*

Application Note: *The SFR FIA_UID.1/PACE in this ST covers the definition in the EAC PP that, in turn, extends the definition in the PACE PP by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.*

6.1.3.3. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1/PACE The TSF shall allow
1. to establish the communication channel,
2. carrying out the PACE Protocol according to [R16-3],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol Version 1 according to [R16-1]71,
6. to carry out the Terminal Authentication Protocol Version 1 according to [R8]72,
7. **to carry out the Active Authentication mechanism**

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

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

***Application Note**: The SFR FIA_UAU.1/PACE in this ST covers the definition in the EAC PP that, in turn, extends the definition in the PACE PP by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.*

***Application Note**: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-KMAC, PACE-KENC), cf. FTP_ITC.1/PACE.*

6.1.3.4. Single-use authentication mechanisms (FIA_UAU.4)

FIA_UAU.4.1/PACE The TSF shall prevent reuse of authentication data related to
1. PACE protocol,
2. Terminal Authentication Protocol,
3. Authentication Mechanism based on ***AES and TDES***,
4. *Active Authentication Protocol*.

***Application note:** The SFR FIA_UAU.4.1 in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from PACE PP.*

6.1.3.5. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1/PACE The TSF shall provide
1. PACE protocol,
2. Passive authentication
3. Terminal Authentication Protocol,
4. Secure messaging in MAC-ENC mode,
5. Symmetric Authentication Mechanism based on ***TDES and AES***

to support user authentication.

FIA_UAU.5.2/PACE The TSF shall authenticate any user's claimed identity according to the following rules:
1. The TOE accepts the authentication attempt as Personalization Agent by *the Symmetric Authentication Mechanism with Personalization Agent Key*.
2. The TOE accepts the authentication attempt as Travel Document Manufacturer by *the Authentication Mechanism with Travel Document Manufacturer Keys*
1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol
2. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
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.

***Application note:** Depending on the authentication methods used the Personalization Agent holds a key for the Symmetric Authentication Mechanism. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication*

between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

6.1.3.6. Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1/EAC 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.

Application note: *The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [15] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.*

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the PACE terminal.

Application note: *The PACE protocol specified in [R16-3] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.*

6.1.3.7. Authentication Proof of Identity (FIA_API.1)

→ Chip Authentication Protocol

FIA_API.1.1/CAP The TSF shall provide a Chip Authentication Protocol according to [16-1] to prove the identity of the TOE.

Application note: *This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [16-1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [15], 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).*

→ Active Authentication Protocol

FIA_API.1.1/AAP The TSF shall provide an *Active Authentication Protocol according to [15]* to prove the identity of the *TOE*.

Application note: *The TOE may implement the Active Authentication Mechanism specified in [15] Part 1 Appendix 4 to section IV. This mechanism is a challenge response protocol where TOE challenge response is calculated being digital signature over the terminal's 8 bytes nonce.*

6.1.4. User data protection (FDP)

6.1.4.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1/ TRM The TSF shall enforce the Access Control SFP on terminals gaining write, read and modification access to data in the EF.SOD of the logical MRTD.

6.1.4.2. Security attribute based access control (FDP_ACF.1)

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

1. Subjects:
   a. BIS-PACE,
   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. all TOE intrinsic secret cryptographic keys stored in the travel document,
3. Security attributes:
   a. PACE authentication
   b. authentication status of terminals,
   c. Terminal Authentication.

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

A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [R16-3] after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

FDP_ACF.1.4/ TRM 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. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel Document
3. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
5. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM
6. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM
7. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application note: *The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [16-1], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.*

***Application Note**: The SFR FDP_ACF.1.1/TRM in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [R7]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP*
***Application Note:** FDP_UCT.1/TRM and FDP_UIT.1/TRM 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 Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).*
***Application Note**: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.*

6.1.4.1. Residual Information Protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable **upon the deallocation of the resource from** the following objects.

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem-SKPICC-PACE (by having generated a DH shared secret K).

6.1.4.2. Basic data exchange confidentiality (FDP_UCT.1)

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

6.1.4.3. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ TRM 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.

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

6.1.4.4. Specifications of Management Functions (FMT_SMF.1)

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

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

6.1.4.5. Security roles (FMT_SMR.1)

FMT_SMR.1.1/ PACE The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal
4. PACE authenticated BIS-PACE
5. Country Verifying Certification Authority,

6. Document Verifier,
7. Basic Inspection Sytem
8. domestic Extended Inspection System
9. foreign Extended Inspection System.

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

***Application Note**: The SFR FMT_SMR.1.1/PACE in this ST covers the definition in the EAC PP that, in turn, extends the definition in PACE PP by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.*

***Application note:** For explanation on the role Manufacturer and Personalisation Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the travel document presenter).*
The TOE recognises the travel document holder or an authorised other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (FIA_UAU.1/PACE)..

6.1.5. Security management (FMT)

6.1.5.1. Limited capabilities (FMT_LIM.1)

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

6.1.5.2. Limited availability (FMT_LIM.2)

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow,
1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

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

6.1.5.3. Management of TSF data (FMT_MTD.1)

→ Writing of Initialization Data and Pre-personalization Data

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

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

→ Disabling of Read Access to Initialization Data and Pre-personalization Data

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

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

→ Initialization of CVCA Certificate and Current Date

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 Verifying Certification Authority Certificate,
3. initial Current Date

to the Personalization Agent.

Application note: *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [16-1], section 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.*

→ Country Verifying Certification Authority

FMT_MTD.1.1/ CVCA_UPD: The TSF shall restrict the ability to update the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate,

to Country Verifying Certification Authority.

Application 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. [16-1], 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. [16-1], sec. 2.2.3 and 2.2.4).*

→ Current date

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.

Application note: *The authorized roles are identified in their certificate (cf. [16-1], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [16-1], annex A.3.3, for details).*

→ Key Write

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

Application 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.*

→ Chip Authentication Private Key

FMT_MTD.1.1/ CAPK — The TSF shall restrict the ability to *load or generate* the Chip Authentication Private Key to *the Personalization Agent*.

Application note: *The component FMT_MTD.1/CAPK was refined in this Security Target by selecting both "create" and "load" operations. The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory: the generator, the modulus and the order. The verb "create" means here that the Chip Authentication Private Key order is generated by the TOE itself. See the instantiation of the component FCS_CKM.1/PK as SFR for this key generation.*

→ Active Authentication Private Key

FMT_MTD.1.1/ AAPK — The TSF shall restrict the ability to *load or generate* the *Active Authentication Private Key* to *the Personalization Agent*.

Application note: *Two operations are selected here and may be used by the successfully authenticated Personalization Agent if he is willing to include the optional Active Authentication Key in the MRTD. The verb "load" means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb "create" means here that the Personalization Agent is requesting the creation of the Active Authentication Key on the TOE and is requesting its secure generation by the TOE itself. See the instantiation of the component FCS_CKM.1/PK as SFR for this key generation.*

→ Personalization agent

FMT_MTD.1.1/ PA — The TSF shall restrict the ability to *write* the *SOD* to *the personalization agent*

→ Key Read

FMT_MTD.1.1/ KEY_READ — The TSF shall restrict the ability to read the
1. PACE passwords
2. Chip Authentication Private Key,
3. Personalization Agent Keys
4. *Active Authentication Private Key*

to none.

6.1.5.4. Secure TSF data (FMT_MTD.3)

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.

Application 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. Protection of the TSF (FPT)

6.1.6.1. TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information of IC Power consumption* in excess of *State of the Art values* enabling access to *Personalization Agent Key(s) and Chip Authentication Private Key, the ephemeral private keys SKpiccc PACE, PACE session keys, chip authentication session keys* and *Active Authentication Private Key*.

FPT_EMSEC.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts *to gain ac*cess to *Personalization Agent Key(s) and Chip Authentication Private Key, the ephemeral private keys SKpiccc PACE, PACE session keys, chip authentication session keys* and *Active Authentication Private Key*.

Application note: *The TOE prevents 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 provides 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.*

6.1.6.2. Failure with preservation of secure state (FPT_FLS.1)

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.

6.1.6.3. Resistance to physical attack (FPT_PHP.3)

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

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

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

6.1.6.4. TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 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.

Application note: *self-test for the verification of the integrity of stored TSF executable code are executed during initial start-up in the Phase 3 "Personalization" and Phase 4 "Operational Use".*

6.1.6.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/ PACE The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ PACE The TSF shall permit another trusted IT product to initiate communication via the trusted channel..

FTP_ITC.1.3/ PACE The TSF shall enforce communication via the trusted channel for any data exchange between the TOE and the Terminal.

6.2. TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 6.2 of the claimed PP [5-1].

ALC_DVS is augmented from 1 to 2, and AVA_VAN is augmented from 3 to 5, compared to the CC V3.1 package for EAL5.

6.2.1. SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete Semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semi-formal modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.2	Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5**	**Advanced methodical vulnerability analysis**

Table 2 – Assurance Requirements: EAL5 augmented

6.2.2. SARs Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 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.

Augmentation results from the selection of:

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

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

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

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 fulfil the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OT.AA_Proof.

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
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures

All of these are met or exceeded in the EAL5 assurance package.

6.3. Security Requirements Rationale

6.3.1. Security Requirement Coverage

The following table associates the security requirements and the security objectives of the TOE. The security requirements of the TOE correspond to at least one security objective of the TOE. Moreover, some requirements correspond to the security objectives of the TOE in combination with other objectives.

TOE SFR / TOE Security objectives	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.AA_Proof	OT.AC_Pers	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				X				X					
FCS_CKM.1/CA	X	X		X	X	X	X						
FCS_CKM.1/DH_PACE					X	X	X						
FCS_CKM.1/KP			X										
FCS_CKM.4	X			X	X	X	X						
FCS_COP.1/CA_ENC	X	X		X	X		X						
FCS_COP.1/CA_MAC	X	X		X	X								
FCS_COP.1/SIG_VER	X			X									
FCS_COP.1/SIG_GEN			X	X									
FCS_COP.1/SHA	X	X	X		X								
FCS_COP.1/PACE_ENC							X						
FCS_COP.1/PACE_MAC					X	X							
FCS_RND.1	X			X	X	X	X						
FIA_AFL.1/PACE											X		
FIA_UID.1/PACE	X			X	X	X	X						
FIA_UAU.1/PACE	X			X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X						
FIA_UAU.5/PACE	X			X	X	X	X						
FIA_UAU.6/EAC	X			X	X	X	X						
FIA_UAU.6/PACE					X	X	X						
FIA_API.1/CAP		X											
FIA_API.1/AAP			X										
FDP_ACC.1/TRM	X			X	X		X						
FDP_ACF.1/TRM	X			X	X		X						
FDP_RIP.1					X	X	X						
FDP_UCT.1/TRM	X				X		X						
FDP_UIT.1/TRM					X		X						
FMT_SMF.1		X		X	X	X	X	X					
FMT_SMR.1/PACE		X		X	X	X	X	X					
FMT_LIM.1									X				
FTM_LIM.2									X				
FMT_MTD.1/INI_ENA				X				X					
FMT_MTD.1/INI_DIS				X				X					

TOE SFR / TOE Security objectives	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.AA_Proof	OT.AC_Pers	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FMT_MTD.1/CVCA_INI	X												
FMT_MTD.1/CVCA_UPD	X												
FMT_MTD.1/DATE	X												
FMT_MTD.1/KEY_WRITE	X			X									
FMT_MTD.1/CAPK	X	X			X								
FMT_MTD.1/AAPK			X	X									
FMT_MTD.1/PA				X	X	X	X						
FMT_MTD.1/KEY_READ	X	X		X	X	X	X						
FMT_MTD.3	X												
FPT_EMSEC.1				X						X			
FPT_FLS.1										X			X
FPT_PHP.3										X		X	
FPT_TST.1										X			X
FTP_ITC.1/PACE					X	X	X				X		

Table 3 – Functional Requirement to TOE Security Objective Mapping

6.3.2. Security Requirements Sufficiency

6.3.2.1. TOE Security Requirements Sufficiency

OT.AA_Proof (Proof of MRTD's chip authenticity by Active Authentication) is ensured by the Active Authentication Protocol provided by FIA_API.1/AAP enforcing the identification and authentication of the MRTD's chip. The Active Authentication protocol requires FCS_RND.1 (for the generation of the challenge), and FCS_COP.1/SHA (for the host challenge hashing) and FCS_COP.1/SIG_GEN (for the signature generation). The Active Authentication private Key is used. This TOE secret data is created during Personalization (Phase 3) according to FCS_CKM.1/KP (for Key Pair generation mechanism), and by authorized agent as required by FMT_MTD.1/ AAPK.

OT.AC_Pers (Access Control for Personalization of logical MRTD) addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data (including Active Authentication keys generated with FCS_COP.1/SIG_GEN) loaded through FMT_MTD.1/AAPK). The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.
The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the

Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use. The Personalization Agent also handles the security environment object according to the SFR FMT_MTD.1/KEY_WRITE.

OT.Data_Int (Integrity of personal data) data" requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.
Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).
The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret andfor the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_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. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

OT.Data_Conf (Confidentiality of personal data) aims that the TOE always ensuresconfidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KENC). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related. 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/TRM and

FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER. The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 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/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_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.
The Personalization Agent manages the security environment object data required for Chip Authentication and for Terminal Authentication according to SFR FMT_MTD.1/KEY_WRITE.
To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.
The security objective OT.Chip_Auth_Proof "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA 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 v.1 [R8] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Data_Aut (Authenticity of personal data) aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Tracing (Tracing travel document) aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:

ii. while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
iii. for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) – FTP_ITC.1/PACE.

OT.Sens_Data_Conf (Confidentiality of sensitive biometric reference data) is enforced by the Access Control SFP defined in FDP_ACC.1 and FDP_ACF.1 allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS_COP.1/SIG_VER. The SFR FIA_UID.1 and FIA_UAU.1 requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the

protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4.
The SFR FIA_UAU.6 and FDP_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/DH (for the generation of shared secret), FCS_CKM.1/CA (for the derivation of the new session keys), and FCS_COP.1/ENC 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 (Identification and Authentication of the TOE) addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. 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 Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cyclephase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Chip_Auth_Proof (Proof of MRTD's chip authenticity) is ensured by the Chip Authentication Protocol provided by FIA_API.1/CAP proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/CA 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 [26] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/ENC and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

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 (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 SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE which is addressed by SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by SFR FPT_PHP.3.

OT.Prot_Phys-Tamper (Protection against Physical Tampering) is covered by the SFR FPT_PHP.3.

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

6.3.3. SFR Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_SAS.1	No dependencies
FCS_CKM.1/CA	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC and FCS_CKM.4

FCS_CKM.1/DH_PACE	A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4
FCS_CKM.1/KP	FCS_COP.1/SIG_GEN, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.1/KP and FCS_CKM.1/CA
FCS_COP.1/CA_ENC	CS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/CA_MAC	CS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/SIG_VER	CS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/SIG_GEN	FCS_CKM.1/KP, FCS_CKM.4 and FCS_CKM.1/CA
FCS_COP.1/SHA	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., FCS_CKM.4
FCS_COP.1/PACE_ENC	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_RND.1	No dependencies
FIA_AFL.1/PACE	FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies
FIA_UAU.1/PACE	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies
FIA_UAU.5/PACE	No dependencies
FIA_UAU.6/EAC	No dependencies
FIA_UAU.6/PACE	No dependencies
FIA_API.1/CAP	No dependencies
FIA_API.1/AAP	No dependencies
FDP_ACC.1/TRM	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1/TRM
FDP_RIP.1	No dependencies
FDP_UCT.1/TRM	FTP_ITC.1/PACE and FDP_ACC.1/TRM
FDP_UIT.1/TRM	FTP_ITC.1/PACE and FDP_ACC.1/TRM
FMT_SMF.1	No dependencies
FMT_SMR.1/PACE	FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2
FTM_LIM.2	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1/ CVCA_INI, FMT_MTD.1/ CVCA_UPD
FPT_EMSEC.1	No dependencies
FPT_FLS.1	No dependencies
FPT_PHP.3	No dependencies
FPT_TST.1	No dependencies
FTP_ITC.1/PACE	No dependencies

Table 4 – SFR Dependencies

7. TOE summary specification

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation.

7.1. SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization and data communication required are satisfied.

7.2. SF.Card Personalization

This TSF provides MRTD's chip personalization functions to allow the Personalization Agent to create and set the initial MRTD's LDS data.

7.3. SF.Personalizer Authentication

The Personalization Agent is authenticated by the TOE.

7.4. SF.PACE

The Basic Access System and the travel document mutually authenticate by means of a Basic Access Control mechanism.

7.5. SF.Chip Authentication

This TSF provides the Chip Authentication protocol to allow the Extended Inspection System to authenticate the TOE.

7.6. SF.Terminal Authentication

This TSF provides Terminal Authentication to allow the TOE to authenticate the terminal using the public authentication material that is presented during the Chip Authentication protocol (DH or ECDH), enforcing the Secure Messaging session.

7.7. SF.Active Authentication

Active Authentication is provided by this TSF based on the availability of DG15 in the MRTD's chip information data.

7.8. SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.

7.9. SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing.

7.10. SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality.

8. Additional Rationale

8.1. SAR Dependencies Rationale

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Requirement	Dependencies
ADV_ARC.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_TDS.4, ADV_IMP.1
ADV_IMP.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5
AGD_OPE.1	ADV_FSP.5
AGD_PRE.1	No dependencies
ALC_CMC.4	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DEL.1	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies
ALC_TAT.2	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies
ASE_TSS.1	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.2
ATE_IND.2	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

Table 5 – SAR Dependencies

8.2. Rationale for Extensions

Extensions are based on the Protection Profile [5-1] and have all been adopted by the developer of the TOE:

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FIA_API.1 ‘Authentication Proof of Identity’
- FPT_EMSEC.1 ‘TOE emanation’
- FMT_LIM.1 and FMT_LIM.2 ‘limited capability and availability’

8.3. Assurance Measures Rationale

Each assurance requirement is covered by an assurance measure.

Assurance Requirements / Assurance Measures	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ADV	X				
AGD		X			
ALC			X		
ATE				X	
AVA					X

Table 6 – Mapping Assurance Requirements to Assurance Measures

8.4. PP Claim Rationale

This ST includes all the security objectives and requirements claimed by PPd [5-1] and [5-2], and, all of the operations applied to the SFRs are in accordance with the requirements of this PP.

The TOE type is compliant with the claimed PPs: the TOE is an ICAO MRTD's chip providing all means of identification and authentication of the TOE itself, the MRTD's traveler and possibly the Terminal.

The TOE is compliant with the representation provided in the ICAO Machine Readable Travel Document Chip with Extended Access Control PP [5-1] and PACE PP [5-2].

The compliance is strict: the addition of specific TOE security mechanisms to the security principles of this Security Target required only the addition of four TOE Objectives related to Active Authentication.

These additions do not affect the concept defined in the PP [5-1] and this ST is a suitable solution to the generic security problem described in the PP.

9. Terminology

Term	Definition
Active Authentication	Security mechanism defined in [15] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs 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 (BAC)	Security mechanism defined in [15] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [15]
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.
CAN (Card Access Number)	Password derived from a short number printed on the front side of the data-page.
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 level 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. [15]
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 State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [15], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Term	Definition
Document Basic Access Keys	Pair of symmetric (two-key) TDES 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 [15]. 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). [15]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [15]
Extended Access Control	Security mechanism identified in [15] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [15]
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. [15]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.

Term	Definition
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. [15]
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. [15]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf.0, TOE lifecycle phase 2 step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [15]
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). [15]
Issuing State	The Country issuing the MRTD. [15]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [15]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [15] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to): (1) personal data of the MRTD holder, (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or 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. [15]

Term	Definition
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. [15]
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. [15]
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. [15]
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 [15], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.
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.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [4],. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. 0, TOE lifecycle phase 3 step 6).

Term	Definition
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent.
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 other data
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. 0, TOE lifecycle phase 2 step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between lifecycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the Traveler is applying for entry. [15]
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. [15]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 Skimming Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel.
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.
Un-personalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF.

Term	Definition
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. [15]
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.

10. References

[1] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-001 - Part 1: Introduction and general model, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-002 -Part 2: Security functional requirements, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation - CCMB-2012-09-003 -Part 3: Security assurance requirements, Revision 4, September 2012.

[4] BSI-CC-PP0055 – Protection Profile — Machine Readable Travel Document with "ICAO Application", Basic Access Control – EAL 4+ – Version: 1.10, 25th March 2009

[5-1] BSI-CC-PP0056-V2-2012 – Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) – EAL 4+ – Version: 1.3.0, 20th January 2012

[5-2] BSI-CC-PP0068-V2-2011 – Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) – EAL 4+ – Version: 1.0, 2nd November 2011

[6] NXP P60D080JVC Technical Datasheet

[7] NXP SmartMX2 Technical Datasheet

[8] BSI-PP-0035-2007 – Security IC Platform Protection Profile – version 1.0 – EAL4+

[9] Certification Report BSI-DSZ-CC-0897-V2-2014 – for NXP Secure Smart Card Controller P60D080/052/040yVC – NXP Semiconductors Germany GmbH – v1.0

[10] NXP Secure Smart Card Controller P60D080/052/040yVC Security Target Lite – Rev 1.3 – 17 October 2013

[11] PKCS#1: RSA Cryptography Standard, Version 1.5

[12] Specifications for the Java Card 3 Platform, Version 3.0.4 Classic Edition, Sept. 2011

- Virtual Machine Specification [JCVM]

- Application Programming Interface [JCAPI]

- Runtime Environment Specification [JCRE]

[13] GlobalPlatform, Card Specification, Version 2.2.1, Jan. 2011 [GPC_SPE_034]

- GlobalPlatform Card ID Configuration, Version 1.0, Dec. 2011 [GPC_GUI_039]

- Confidential Card Content Management – Amendment A, v1.0.1, Jan 2011

- Secure Channel Protocol 03 – Amendment D, v1.1, Sept. 2009

[14] CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007

[15] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[16-1] TR-03110, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, BSI

[16-2] ICAO: Supplement to doc 9303 – Release 11 – November 17, 2011

[16-3] ICAO: Technical report supplemental access control for machine readable travel documents – Version 1.01 – November 11, 2010

[16-4] Technical Guideline TR-03110-3, Advanced Security Mechanisms forMachine Readable Travel Documents – Part 3 – Common Specifications, Version 2.10, 20. March 2012

[17] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques

based on elliptic curves — Part 3: Key establishment, 2002

[18] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

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

[20] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[21] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[22] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[23] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography

[24] ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999

[25] NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197-2001

[26] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, special publication 800-38B-2005