IDENTITY & SECURITY

SECURITY TARGET LITE
FOR IDEAL PASS V2.0.1
EAC WITH PACE APPLICATION

Reference: 2016_2000023040

Date	Version	Revision
01/12/2016	1.0	Document creation

Table of contents

Table of figures

Table of tables

1 Introduction

1.1 Security Target Lite and TOE reference

ST reference :		
Title	:	Security Target Lite for IDeal PASS V2.0.1 EAC with PACE application
Version	:	1.0
Security target identifier	:	2016_2000023040
TOE reference :		
Chip identifier	:	Infineon M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)
Masked chip reference	:	IDealPass_v2.0.1N_M7892_1_0_0
Crypto library		Toolbox v1.02.013
Chip Component Assurance Level		EAL6+, augmented with ALC_FLR.1
TOE Identifier		IDEALPASSV201SAC/EAC_NTePASSPORT/1.0.0
Administration guidance	:	**2016_2000017817 - Preparative Procedures**
User guidance	:	**2016_2000017816 - Operational User Guidance**
CC compliance :		
Version	:	3.1
Assurance level	:	EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5
Chip and cryptolibrary certificate reference	:	M7892 : BSI-DSZ-CC-0782-V2-2015
Protection Profile		BSI-CC-PP-0056-V2-2012 MA-02 [R7] BSI-CC-PP-0068-V2-2011-MA-01 [R16]

1.2 TOE Overview

The security target lite defines the security objectives and requirements for the contact based / contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment, Extended Access Control, and Chip Authentication similar to the Active Authentication in 'ICAO Doc 9303' [R6].

1.2.1 TOE definition

The Target of Evaluation (TOE) addressed by the current protection profile is an electronic travel document representing a contactless / contact smart card programmed according to ICAO Technical Report "Supplemental Access Control" [R7] (which means amongst others according to the Logical Data Structure (LDS) defined in [R6])and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [R6] and BSI TR-03110 [R5], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-MA-01 [R16].

The TOE comprises of at least

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

1.2.2 TOE usage and security features for operational use

A State or Organisation issues travel documents to be used by the holder for international travel. The traveller presents a travel document to the inspection system to prove his or her identity. The travel document in context of this protection profile 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 travel document's chip according to LDS in case of contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.
For this protection profile the travel document is viewed as unit of

i. The **physical part of the travel document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
   a) the biographical data on the biographical data page of the travel document surface,
   b) the printed data in the Machine Readable Zone (MRZ) and
   c) the printed portrait.
ii. The **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [R6] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document 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[1]
d) the other data according to LDS (EF.DG5 to EF.DG16) and
e) the Document Security Object (SOD).

The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [R7]. These security measures can include the binding of the travel document's chip to the travel document.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [R6], and Password Authenticated Connection Establishment'. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This protection profile addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This protection profile addresses the Chip Authentication Version 1 described in [R9] as an alternative to the Active Authentication.

If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [R8] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

The confidentiality by Password Authenticated Connection Establishment (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 [R4], 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.

[1] These biometric reference data are optional according to [6]. This PP assumes that the issuing State or Organisation uses this option and protects these data by means of extended access control.

iii. The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.

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

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [R9].

The security target requires the TOE to implement the Extended Access Control as defined in [R5]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 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 v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation 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 Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.2.3 TOE Boundary

The Target Of Evaluation (TOE) is the contact/contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing Basic Access Control and Extended Access Control according to the ICAO Doc 9303 [R6]. The TOE may also provide Active Authentication accordin to [R6].

The TOE boundary encompasses:

- The ICAO application
- The Active Authentication mechanism according to the ICAO document [R6]
- The Operating System
- The Infineon embedded crypto library : Toolbox v1.02.013
- The Infineon chip: Infineon M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)

The TOE does not allow any additional applets loading during its operational use.

1.2.4 Product architecture

The Product is embedding two applications:

- NSD (Native Security Domain) Application insures card security during application personalization. This application is not accessible once in Operational Use phase.
- The ICAO application, which is compliant with [R4] [R5] [R6] . The ICAO application may be instantiated several times.

The product does not allow any additional applets loading during its operational use.

The architecture of the IDeal Pass v2.0.1 is given in Figure 1.

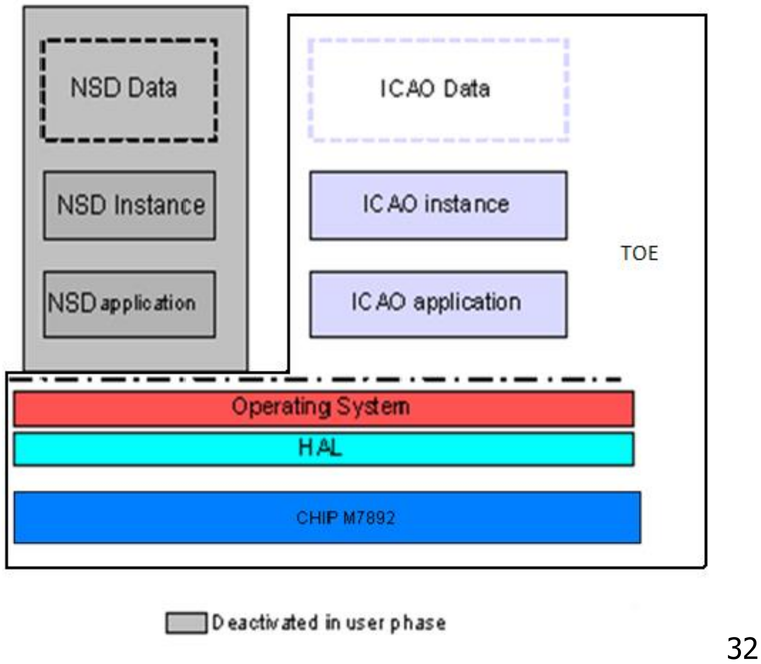


Figure 1: Architecture of the IDeal Pass v2.0.1

1.2.5 TOE life cycle

The product's life cycle is organised as follows:

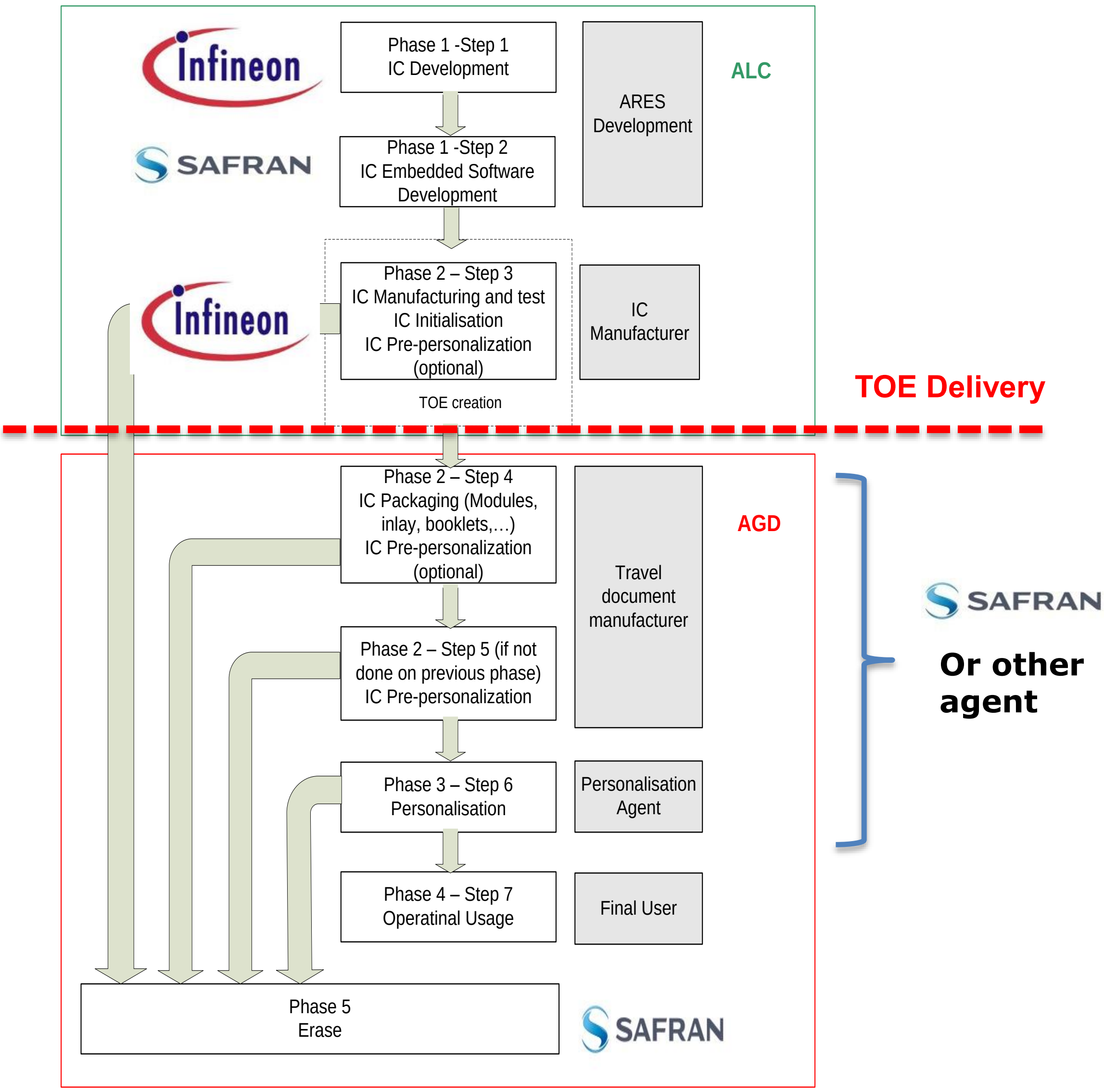


Figure 2: TOE life cycle

The table below presents the TOE role:

Roles	Actors
IC Developer	Infineon
IC Manufacturer	Infineon

Roles	Actors
TOE Developer	Safran Identity & Security (OSNY-France – Development) Safran Identity & Security (NOIDA-India – Qualification/Testing only)
Travel Document Manufacturer	Safran Identity & Security Or another agent
Personalization Agent	Safran Identity & Security Or another agent

The table below presents the Actors following TOE life cycle steps in accordance with the standard smart card life cyce and the Protection Profile lifecycle phases, the TOE delivery point and the coverage:

Step/Phase	Actors	Sites	Covered by
Phase 1-Step 1	Infineon	Dresden	ALC (IC certification)
Phase 1-Step 2	Safran Identity & Security	Osny (development) and Noida (Qualification/Testing)	ALC R&D site ALC Qualification site
Phase 2-Step 3	Infineon	Dresden	ALC (IC certification)
TOE Delivery			
Phase 2-Step 4	Travel Document Manufacturer		AGD_PRE
Phase 2-Step 5	Travel Document Manufacturer		AGD_PRE
Phase 3-Step 6	Personalizer		AGD_PRE
Phase 4-Step 7	End User		AGD_OPE

The TOE life cycle is described in the following table:

Phase Number	Phase name	Description / Authority
1	Development	(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components. (Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components. The Safran Identity & Security ePassport code is securely delivered directly from the software developer (Safran Identity & Security.) to the IC manufacturer (Infineon).
2	Manufacturing	(Step3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (FLASH). 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 ePassport application code will be integrated in the FLASH memory by the IC manufacturer. (Step 4) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), (iii) the Document security object. The signing of the Document security object by the Document Signer [R9] 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. This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [R9]. This approach allows but does not enforce the separation of these roles.
3	Personalization agent	(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary.
4	Operational Use	(Step 7) The TOE is used as MRTD's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the Issuing State or Organization and can be used according to the security policy of the Issuing State but they can never be modified

5	Erase	The erase function is included into the TOE. The access to this function is granted only and only if Mutal Authentication with Key set n°1 is successful. After the erase all TOE data (Sensitive and non sensitive) are Erased. Infineon Bootloader will be re-activated. The erase function is not accessible after Phase 3 (Operational Usage)

2 Conformance Claims

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4 [R2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4 [R3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4 [R10] has to be taken into account.

2.2 ST Claim

This ST claims strict conformance to

- *Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2 MA-02 [R7],*

Since the PP above claim strict conformance to [R16], this ST implicitly also claims strict conformance to:

- *"Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)", BSI-CC-PP-0068-V2-2011-MA01, Version 1.01, 22.07.2014, [R16].*

The following elements have been added for the optional Active Authentication mechanism according to [R6]:

- Objectives for the TOE:
  - OT.Chip_Auth_Proof
- SFRs:
  - FCS_COP.1/SIG_GEN
  - FIA_API.1/AAP
  - FMT_MTD.1/AAPK

2.3 Package Claim

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [R3].

2.4 Conformance rationale

This ST claims strict conformance to [R7]. [R7] claiming strict conformance to [R16], this ST also claims strict conformance to [R16]. This has the following implications:

1. The TOE type of this ST is the same as the TOE type of the claimed PPs: the Target of Evaluation (TOE) is a smart card programmed according to [R5], [R6] and [R4], and named a travel document as a whole.
2. The security problem definition (SPD) of this ST contains the SPD of the claimed PPs. Hence, the SPD of this ST contains all threats, organizational security policies and assumptions of the claimed PPs.
3. The security objectives for the TOE in this ST include all security objectives for the TOE of the claimed PPs.
4. The security objectives for the operational environment in this ST include all security objectives for the operational environment of the claimed PPs.
5. The security functional requirements (SFRs) specified in this ST include all SFRs specified in the claimed PPs.
6. The security assurance requirements (SARs) specified in this ST (EAL5+) are augmented with ADV_FSP.5, ADV_TDS.4, ADV_INT.2, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3 compared to the SARs specified in the claimed PP (EAL4+).

3 Security problem definition

3.1 Assets

3.1.1 PP-0056

The assets to be protected by the TOE include the User Data on the travel document's chip, user data transferred between the TOE and the terminal, and travel document tracing data from the claimed EAC PP [R7].

3.1.1.1 Assets listed in PP PACE

Due to strict conformance to PACE PP, this PP also includes all assets listed in [R16], namely the primary assets user data stored on the TOE (object 1), user data transferred between the TOE and the terminal connected (object 2), travel document tracing data (object 3), and the secondary assets accessibility to the TOE functions and data only for authorised subjects (object 4) Genuineness of the TOE (object 5), TOE intrinsic secret cryptographic keys (object 6), TOE intrinsic non secret cryptographic material (object 7), and travel document communication establishment authorisation data (object 8).

user data stored on the TOE

All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [R4] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R4]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [R9].

The generic security properties to be maintained by the current security policy are:

Confidentiality (Though not each data element stored on the TOE represents a secret, the specification [R4] anyway requires securing their confidentiality: only terminals authenticated according to [R4] can get access to the user data stored. They have to be operated according to P.Terminal.)

Integrity

Authenticity

user data transferred between the TOE and the terminal connected

The terminal connected is an authority represented by Basic Inspection System with PACE.

All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [R4] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R4]). User data can be received and sent (exchange means receive and send).

The generic security properties to be maintained by the current security policy are:

Confidentiality (Though not each data element being transferred represents a secret, the specification [R4] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [R4])

Integrity

Authenticity

travel document tracing data

Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PAC E password. TOE tracing data can be provided / gathered.

The generic security property to be maintained by the current security policy is:

Unavailability (it represents a prerequisite for anonymity of the travel document holder)

Accessibility to the TOE functions and data only for authorised subjects

Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.

The property to be maintained by the current security policy is:

Availability

Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [R9].

The property to be maintained by the current security policy is:

Availability

TOE internal secret cryptographic keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

The properties to be maintained by the current security policy are:

Confidentiality

Integrity

TOE internal non-secret cryptographic material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

The properties to be maintained by the current security policy are:

Integrity

Authenticity

travel document communication establishment authorisation data

Restricted-revealable (The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy) authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.

The properties to be maintained by the current security policy are:

Confidentiality

Integrity

Application note:

Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

The travel document communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt. The TOE shall secure the reference information as well as 'together with the terminal connected (the input device of the terminal)' the verification information in the 'TOE - terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE.

3.1.1.2 Additional Assets

Logical travel document sensitive User Data

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

Application note:

Due to interoperability reasons the 'ICAO Doc 9303' [R6] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC [R6]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [R8]). If supported, it is therefore recommended to used PACE instead of BAC. *If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks*

Authenticity of the travel document's chip

The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.

3.2 Users / Subjects

3.2.1 PP-0056

This protection profile considers the following subjects additionally to those defined in PACE PP [R16]:

3.2.1.1 Subjects listed in PP PACE

This PP includes all subjects from the PACE Protection Profile [R16], namely Manufacturer, Personalisation Agent, Basic Inspection System (with PACE), Document Signer (DS), and Country Signing Certification Authority (CSCA), Travel Document Holder and Travel Document Presenter (traveller).

Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [R9].

Personalisation Agent

An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [R6], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [R6] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [R9].

Basic Inspection System with BIS-PACE

A technical system being used by an inspecting authority (concretely, by a control officer) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-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.

Document Signer

It is also called DS. An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [R6]. This role is usually delegated to a Personalisation Agent.

Country Signing Certification Authority

It is also called CSCA. An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [R6], 5.5.1.

travel document holder

A person for whom the travel document Issuer has personalised the travel document (i.e. this person is uniquely associated with a concrete electronic Passport). This entity is commensurate with 'MRTD Holder' in [R9]. Please note that a travel document holder can also be an attacker (see below).

travel document presenter

It represents the traveler. A person presenting the travel document to a terminal (in the sense of [R4]) and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [R9]. Please note that a travel document presenter can also be an attacker (see below).

3.2.1.2 Additional Subjects

Country Verifying Certification Authority

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

Document Verifier

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

Terminal

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

Inspection system (IS)

It also called IS. A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.

The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [R5] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

Application note:

For definition of **Basic Inspection System (BIS)** resp. Basic Inspection System with PACE (BIS-PACE) see PACE PP [R16].

Attacker

Additionally to the definition from PACE PP [R16], chap 3.1 the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document.

Application note:

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

3.3 Threats

3.3.1 PP-0056

This section describes the threats to be averted by the TOE independently or in collaboration environment and the assets stored in or protected by the TOE.

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

3.3.1.1 Threats listed in PP PACE

This PP includes all threats from the PACE PP [R16], chap 3.2, namely T.Skimming, T.Eavesdropping, T.Tracing, T.Abuse-Func, T.Information_Leakage, T.Phys-Tamper, T.Forgery and T.Malfunction.

T.Forgery from the PACE PP [R16] shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

T.Skimming

Skimming travel document / Capturing Card-Terminal Communication

Adverse action: 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.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel documentdata

Application note:

A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP.

MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder.

T.Eavesdropping

Eavesdropping on the communication between the TOE and the PACE terminal

Adverse action: 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*.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel documentdata

Application note:

A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this PP.

T.Tracing

Tracing travel document

Adverse action: 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.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: privacy of the travel document holder

Application note:

This Threat completely covers and extends 'T.Chip-ID' from BAC PP [R9].

A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this PP.

T.Forgery

Forgery of Data

Adverse action: 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.

Threat agent: having high attack potential

Asset: integrity of the travel document

Application note:

T.Forgery shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

T.Abuse-Func

Abuse of Functionality

Adverse action: 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.

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

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document

Application note:

Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage

Information Leakage from travel document

Adverse action: 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.

Threat agent: having high attack potential.

Asset: confidentiality of User Data and TSF-data of the travel document

Application note:

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

T.Phys-Tamper

Physical Tampering

Adverse action: 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.

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

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application note:

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

T.Malfunction

Malfunction due to Environmental Stress

Adverse action: 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.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

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 threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

3.3.1.2 Additional Threats

T.Read_Sensitive_Data

Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [R8]) 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.

Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document.

Asset: confidentiality of logical travel document sensitive user data(i.e. biometric reference)

T.Counterfeit

Counterfeit of travel document chip data

Adverse action: 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.

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

Asset: authenticity of user data stored on the TOE

Application note:

Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE. T.Counterfeit might be formulated like: 'An attacker produces an unauthorised copy or reproduction of a genuine travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of an travel document presenter as the travel document holder'.

3.4 Organisational Security Policies

3.4.1 PP-0056

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

3.4.1.1 OSP listed in PP PACE

This PP includes all OSPs from the PACE PP [R16], chap 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal.

P.Manufact

Manufacturing of the travel document'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.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 TOE.

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.

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 (issuing branch)

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 (C.CSCA).

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 (C.CSCA) having to be made available to the travel document Issuer by strictly secure means, see [R6], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C.DS) and make them available to the travel document Issuer, see [R6], 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.

Application note:

The given description states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

P.Trustworthy_PKI

Trustworthiness of 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

Abilities and trustworthiness of terminals

The Basic Inspection Systems with PACE (BIS-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 as defined in [R6].

2)They shall implement the terminal parts of the PACE protocol [R4], of the Passive Authentication [R6] and use them in this order (This order is commensurate with [R4]). 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 C.CSCA and C.DS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [R6]).

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.

3.4.1.2 Additional OSPs

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.Personalisation

Personalisation of the travel document by issuing State or Organisation only

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.

3.5 Assumptions

3.5.1 PP-0056

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

3.5.1.1 Assumptions listed in PP PACE

This PP includes the assumption from the PACE PP [R16], chap 3.4, namely A.Passive_Auth.

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 according to [R6].

3.5.1.2 Additional Assumptions

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 [R4] and/or BAC [R8]. 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.

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [R16] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

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.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [R16] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 PP-0056

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

4.1.1.1 Security Objectives listed in PP PACE

This PP includes all Security Objectives for the TOE from the PACE PP [R16], chap 4.1, namely OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.Prot_Abuse-Func, OT.Prof_Inf_Leak, OT.Prot_Phys-Tamper, OT.Identification, OT.AC_Pers and OT.Prot_Malfunction.

OT.Data_Integrity

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data (where appropriate) 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_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data (where appropriate) 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.

Application note:

Application note 21: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity) cannot be achieved by the current TOE.

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

Potection against Information Leakage

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

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

Application note:

Application note 22: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's 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 electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, 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 functionality.

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 have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature. The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment*.

OT.Identification

Identification of the TOE

The TOE must provide means to store Initialisation (amongst other, IC Identification data) 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).

OT.Data_Authenticity

Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data (where appropriate), stored on it by enabling verification of their authenticity at the terminal-side (verification of SO.D). 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, secure messaging after the PACE authentication, see also [R4]).

OT.AC_Pers

Access Control for Personalisation 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 [R6] 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.

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 want 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.

Application note:

Application note 23: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

4.1.1.2 Additional Security Objectives

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 the travel document's chip authenticity

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [R5]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application note:

The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document'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 travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [R6] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

4.2 Security objectives for the Operational Environment

4.2.1 PP-0056

4.2.1.1 OE listed in PP PACE

This PP includes all Security Objectives of the TOE environment from the PACE PP [R16], chap. 4.2, namely OE.Legislative_Compliance, OE.Passive_Auth_Sign, OE.Personalisation, OE.Terminal, and OE.Travel_Document_Holder.

OE.Legislative_Compliance

The **travel document Issuer as the general responsible** for the global security policy related will implement this security objectives:

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 and the related CSCA** will implement this security objectives:

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 [R6]. 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.Personalisation

Personalisation of travel document

The **travel document Issuer and the related CSCA** will implement this security objectives:

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 as defined in [R6] (see also [R6], sec. 10), (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [R6] (in the role of a DS).

OE.Terminal

Terminal operating

The terminal operators (terminal's receiving branch) 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 [R6]. 2)The related terminals implement the terminal parts of the PACE protocol [R4], of the Passive Authentication [R4] (by verification of the signature of the Document Security Object) and use them in this order (this order is commensurate with [R4]). 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 C.CSCA and C.DS) 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, [R6]). 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.

Application note:

Application note 24: OE.Terminal completely covers and extends 'OE.Exam_MRTD', 'OE.Passive_Auth_Verif' and 'OE.Prot_Logical_MRTD' from BAC PP [R9].

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.

4.2.1.2 Additional OEs

Issuing State or Organisation

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

OE.Auth_Key_Travel_Document

Travel document Authentication Key

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.

This objective is implemented by the issuing State or Organisation.

Justification: This security objective for the operational environment is needed additionally to those from [R16] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in [R16].

OE.Authoriz_Sens_Data

Authorization 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.

This objective is implemented by the issuing State or Organisation.

Justification: This security objective for the operational environment is needed additionally to those from [R16] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in [R16].

Receiving State or Organisation

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

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 [R4] and/or the Basic Access Control [R6]. 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.

This objective is implemented by the receiving State or Organisation.

Justification: This security objective for the operational environment is needed additionally to those from [R16] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [R16] and therefore also counters T.Forgery and A.Passive_Auth from [R16]. This is done because a new type of Inspection System is introduced in this PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

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.

This objective is implemented by the receiving State or Organisation.

Justification: This security objective for the operational environment is needed additionally to those from [R16] in order to handle the Assumption A. Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

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.

This objective is implemented by the receiving State or Organisation.

Justification: This security objective for the operational environment is needed additionally to those from [R16] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 PP-0056

<u>Threats listed in PP PACE</u>

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_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality 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.

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_Confidentiality through a trusted channel based on the PACE authentication.

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).

T.Forgery 'Forgery of data' 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. Additionally to the security objectives from PACE PP [R16] which counter this threat, 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.Forgery also 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_Integrity and OT.Data_Authenticity, 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.

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.

T.Information_Leakage is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Inf_Leak.

T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Phys-Tamper.

T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is obviously addressed by the directly related security objective OT.Prot_Malfunction.

Additional Threats

T.Read_Sensitive_Data 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'.

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.

4.3.2 Organisational Security Policies

4.3.2.1 PP-0056

OSP listed in PP PACE

P.Manufact 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**.

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'.

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).

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

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 [R16]. OE.Exam_Travel_Document enforces the terminals to perform the terminal part of the PACE protocol.

The OSP P.Terminal is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable.

Additional OSPs

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'.

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.

4.3.3 Assumptions

4.3.3.1 PP-0056

Assumptions listed in PP PACE

A.Passive_Auth The assumption A.Passive_Auth 'PKI for Passive Authentication' is directly covered by the security objective for the TOE environment OE.Passive_Auth_Sign 'Authentication of travel document by Signature' from PACE PP [R16] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_Travel_Document 'Examination of the physical part of the travel document'.

Additional Assumptions

A.Insp_Sys The examination of the travel document addressed by the assumption A.Insp_Sys 'Inspection Systems for global interoperability' is covered by the security objectives for the TOE environment OE.Exam_Travel_Document 'Examination of the physical part of the travel document' which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment OE.Prot_Logical_Travel_Document 'Protection of data from the logical travel document' require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

A.Auth_PKI 'PKI for Inspection Systems' is covered by the security objective for the TOE environment OE.Authoriz_Sens_Data 'Authorization for use of sensitive biometric reference data' requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by OE.Ext_Insp_Systems 'Authorization of Extended Inspection

Systems' to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Skimming	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.Travel_Document_Holder	Section 4.3.1
T.Eavesdropping	OT.Data_Confidentiality	Section 4.3.1
T.Tracing	OT.Tracing, OE.Travel_Document_Holder	Section 4.3.1
T.Forgery	OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper, OE.Personalisation, OE.Passive_Auth_Sign, OE.Terminal, OE.Exam_Travel_Document	Section 4.3.1
T.Abuse-Func	OT.Prot_Abuse-Func	Section 4.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 4.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 4.3.1
T.Malfunction	OT.Prot_Malfunction	Section 4.3.1
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OE.Auth_Key_Travel_Document, OE.Exam_Travel_Document	Section 4.3.1

Table 1 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.Data_Integrity	T.Skimming, T.Forgery
OT.Data_Confidentiality	T.Skimming, T.Eavesdropping
OT.Tracing	T.Tracing
OT.Prot_Abuse-Func	T.Forgery, T.Abuse-Func
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper
OT.Prot_Malfunction	T.Malfunction
OT.Identification	
OT.Data_Authenticity	T.Skimming, T.Forgery
OT.AC_Pers	T.Forgery
OT.Sens_Data_Conf	T.Read_Sensitive_Data
OT.Chip_Auth_Proof	T.Counterfeit
OE.Legislative_Compliance	
OE.Passive_Auth_Sign	T.Forgery
OE.Personalisation	T.Forgery
OE.Terminal	T.Forgery
OE.Travel_Document_Holder	T.Skimming, T.Tracing
OE.Auth_Key_Travel_Document	T.Counterfeit
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data
OE.Exam_Travel_Document	T.Forgery, T.Counterfeit
OE.Prot_Logical_Travel_Document	
OE.Ext_Insp_Systems	T.Read_Sensitive_Data

Table 2 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 4.3.2
P.Pre-Operational	OT.Identification, OT.AC_Pers, OE.Personalisation, OE.Legislative_Compliance	Section 4.3.2
P.Card_PKI	OE.Passive_Auth_Sign	Section 4.3.2
P.Trustworthy_PKI	OE.Passive_Auth_Sign	Section 4.3.2
P.Terminal	OE.Terminal, OE.Exam_Travel_Document	Section 4.3.2
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.2
P.Personalisation	OT.AC_Pers, OT.Identification, OE.Personalisation	Section 4.3.2

Table 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.Data_Integrity	
OT.Data_Confidentiality	
OT.Tracing	
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OT.Identification	P.Manufact, P.Pre-Operational, P.Personalisation
OT.Data_Authenticity	
OT.AC_Pers	P.Pre-Operational, P.Personalisation
OT.Sens_Data_Conf	P.Sensitive_Data
OT.Chip_Auth_Proof	
OE.Legislative_Compliance	P.Pre-Operational
OE.Passive_Auth_Sign	P.Card_PKI, P.Trustworthy_PKI
OE.Personalisation	P.Pre-Operational, P.Personalisation
OE.Terminal	P.Terminal
OE.Travel_Document_Holder	
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	P.Sensitive_Data
OE.Exam_Travel_Document	P.Terminal
OE.Prot_Logical_Travel_Document	
OE.Ext_Insp_Systems	P.Sensitive_Data

Table 4 Security Objectives and OSPs - Coverage

Assumptions	Security objectives for the Operational Environment	Rationale
A.Passive_Auth	OE.Passive_Auth_Sign, OE.Exam_Travel_Document	Section 4.3.3
A.Insp_Sys	OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document	Section 4.3.3
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 4.3.3

Table 5 Assumptions and Security Objectives for the Operational Environment - Coverage

Security objectives for the Operational Environment	Assumptions
OE.Legislative_Compliance	
OE.Passive_Auth_Sign	A.Passive_Auth
OE.Personalisation	
OE.Terminal	
OE.Travel_Document_Holder	
OE.Auth_Key_Travel_Document	
OE.Authoriz_Sens_Data	A.Auth_PKI
OE.Exam_Travel_Document	A.Passive_Auth, A.Insp_Sys
OE.Prot_Logical_Travel_Document	A.Insp_Sys
OE.Ext_Insp_Systems	A.Auth_PKI

Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended requirements

5.1 Extended families

5.2 Definition of the Family FAU_SAS

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

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

FAU_SAS Audit data storage

Family behaviour

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

Component levelling

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional 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 behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use 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*].

5.4 Definition of the Family 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 1: 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. [R3], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

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 levelling

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.5 Definition of the Family FMT_LIM

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

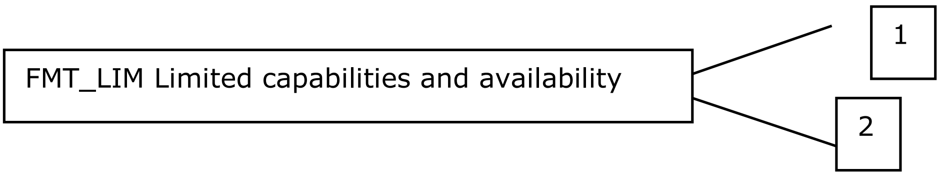
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component levelling



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

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

FMT_LIM.1 Limited capabilities.

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its 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 its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application note 2: 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

– 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

– 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.

5.6 Definition of the Family FPT_EMS

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirement 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 [R2].

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

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling

FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.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_EMS.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 Functional Requirements

6.1 Security Functional Requirements

6.1.1 PP-0056

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [R1]of the CC. Each of these operations is used in this PP.

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

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are italicized.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized like this.

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

Note, that all the subjects used ('Manufacturer', 'Personalisation Agent', 'Extended Inspection System', 'Country Verifying Certification Authority', 'Document Verifier' and 'Terminal') are acting for homonymous external entities. All used objects are defined at the end of the document 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].

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality. SFRs from the PACE PP are not repeated in this PP but listed in Table 4. Only those SFRs from PACE PP extended in this PP are written down below.

SFRs to be taken from PACE PP [R16]
FAU_SAS.1
FCS_CKM.1/DH_PACE
FCS_CKM.4
FCS_COP.1/PACE_ENC
FCS_COP.1/PACE_MAC
FCS_RND.1
FIA_AFL.1/PACE
FIA_UAU.6/PACE
FDP_RIP.1
FDP_UCT.1/TRM
FDP_UIT.1/TRM
FMT_SMF.1
FMT_MTD.1/INI_ENA
FMT_MTD.1/INI_DIS
FMT_MTD.1/PA
FPT_TST.1
FPT_FLS.1
FPT_PHP.3
FTP_ITC.1/PACE

6.1.1.1 SFRs listed in PP PACE

FCS_CKM.1/DH_PACE Cryptographic key generation DH for PACE session key

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie-Hellman Protocol (PKCS3),ECDH (ISO 15946)**4

[R17] and specified cryptographic key sizes **1024, 1536 and 2048 bits and 192, 224 ,256, 320, 384, 512 and 521 bits** that meet the following**: [R10],Annex A.1 and [R13]and [R14]**.

Application note:

The TOE generates a shared secret value K with the terminal during the PACE protocol, see [R4]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R13]) or on the ECDH compliant to TR-03111 [R12] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [R4]and [R12] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K.MAC, PACE-K.Enc) according to [R4]for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R4].

FCS_CKM.4 Cryptographic key destruction

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

Application note:

The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

FCS_COP.1/PACE_ENC Cryptographic operation

FCS_COP.1.1/PACE_ENC The TSF shall perform **secure messaging - encryption and decryption**

in accordance with a specified cryptographic algorithm **3DES and AES in CBC mode** and cryptographic key sizes **respectively 112 and 128, 192 and 256bits** that meet the following: **compliant to** [R4]**.**

Application note:

This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc).

FCS_COP.1/PACE_MAC Cryptographic operation

FCS_COP.1.1/PACE_MAC The TSF shall perform **secure messaging - message authentication code**

in accordance with a specified cryptographic algorithm **Retail-MAC and CMAC** and cryptographic key sizes **respectively 112 and 128, 192 and 256bits**that meet the following: **compliant to** [R4].

Application note:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K.MAC). Note that in accordance with [R4] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **3** unsuccessful authentication attempts occur 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 **consecutively increase the reaction time of the TOE before a new authentication attempt**

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 [R4]) 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'*.

FIA_UAU.6/PACE Re-authenticating

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 [R4] 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.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to and deallocation of the resource from** the following objects: **1. Session Keys (immediately after closing related communication session),**

2. the ephemeral private key ephem - SK PICC- PACE (by having generated a DH shared secret K).

Application note:

The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key-s destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

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

FDP_UCT.1/TRM Basic data exchange confidentiality

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

FDP_UIT.1/TRM Data exchange integrity

FDP_UIT.1.1/TRM The TSF shall enforce the **Access Control SFP** 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.

FTP_ITC.1/PACE Inter-TSF trusted channel

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 initiate communication via the trusted channel for **any data exchange between the TOE and the Terminal. NOTE: the TSF shall enforce instead of initiate**

Application note:

The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word 'initiate' is changed to 'enforce', as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K.MAC, PACE-K.Enc): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

FMT_SMF.1 Specification of Management Functions

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

1. **Initialization,**
2. **Pre-personalisation,**
3. **Personalisation**
4. **Configuration**.

FMT_MTD.1/INI_ENA Management of TSF data

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

Application note:

The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

FMT_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **Document Security Object (SO.D)** to **the Personalisation Agent**.

Application note:

By writing SO.D into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **1. Exposure to operating conditions causing a TOE malfunction,**

2. Failure detected by TSF according to FPT_TST.1,

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

FPT_TST.1 TSF testing

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

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

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

Application note:

If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

FPT_PHP.3 Resistance to physical attack

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

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **initialisation and pre-personnalization data** in the audit records.

Application note:

The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers with a reprocessing algorithmic that meet **AIS31 Class P2 quality metric**.

Application note:

This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalisation Agent**.

Application note:

The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

6.1.1.2 Additional SFRs

Class Cryptographic Support (FCS)

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

Cryptographic operation (FCS_COP.1)

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

FCS_COP.1/SYM Cryptographic operation

FCS_COP.1.1/SYM The TSF shall perform **secure messaging encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES and AES in CBC mode** and cryptographic key sizes **respectively 112 and 128, 192 and 256 bits** that meet the following: **[**[R5]**]**.

Application note:

This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **ECDSA and RSA.**

For ECDSA the cryptographic key sizes are: 192, **224, 256, 320, 384** ,512 **and 521 bits** that meet the following: **ISO15946-2 specified in** 4

[R17] **in combination with SHA1, SHA224, SHA256, SHA384 and SHA512 digest algorithms**

For RSA the cryptographic key sizes are: 1280, **1536, 1792, 2560 and 3072 bits .** that meet the following:**RSA PKCS#1 v1.5 and RSA PSS specified in**

[R18] **in combination with SHA1 and SHA256 digest algorithms for RSA PKCS#1 v1.5 and SHA1 ,SHA256 and SHA512 for RSA PSS**

Application note:

The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal Authentication Protocol v.1 (cf. [R5]). 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.

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging message authentication code** in accordance with a specified cryptographic algorithm **3DES Retail MAC and AES CMAC** and cryptographic key sizes **respectively 112 and 128, 192 and 256bits** that meet the following: [R6]

Application note:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 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.

FCS_COP.1/SIG_GEN Cryptographic operation

FCS_COP.1.1/SIG_GEN The TSF shall perform :

digital signature generation in accordance with a specified cryptographic algorithm **ECDSA and RSA** and cryptographic key sizes **192,224, 256 ,320, 384, 512 and 521 bits for ECDSA and 1536, 1792 ,2048, 2560, and 3072bits for RSA** that meet the following: **ISO15946-2**4

[R17] **for ECDSA and RSA-PKCS#1-v2.1**[R18] **for RSA, in combination with SHA1, SHA224, SHA256, SHA384 and SHA512 digest algorithms for**

ECDSA and SHA1, SHA224, SHA256, SHA384, and SHA512 digest algorithms for ECDSA.

Application note:

This SFR has been added to this ST in order to support the signing of challenges generated by the Inspection System as part of the optional Active Authentication protocol specified in [ICAO-9303].

Miscellaneous

FCS_CKM.1/CA Cryptographic key generation

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on the ECDH protocol and Diffie-Hellman Protocol,** and specified cryptographic key sizes 192, **224, 256, 320, 384, 512 or 521 bits and 2048 bits** that meet the following: **[DH-PKCS#3] and [TR-03111]**.

Application note:

FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R5].

The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [R5]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R12]) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [R13], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [R5]).

The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 (cf. [R5]). The TOE may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [R5] for details).

The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [R16] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

Class FIA Identification and Authentication

The Table 5 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Active Authentication Protocol	FIA_API.1.1/AAP
Authentication Mechanism for Personalisation Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE

Note the Chip Authentication Protocol Version 1 as defined in this protection profile includes:

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 Version 1,

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 Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

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

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow **1. to establish the communication channel,**

2. carrying out the PACE Protocol according to [R4]**,**

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 [R5]

5. to carry out the Terminal Authentication Protocol v.1 according to [R5] 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:

The SFR FIA_UID.1/PACE in the current PP covers the definition in PACE PP [R16] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

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-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 'Personalisation of the travel document'. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. 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 Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

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).

In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow **1. to establish the communication channel,**

2. carrying out the PACE Protocol according to [R4]**,**

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 [R5]

6. to carry out the Terminal Authentication Protocol Version 1 according to [R5] **16** 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 the current PP covers the definition in PACE PP [R16] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

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-K.MAC, PACE-K.Enc), cf. FTP_ITC.1/PACE.

FIA_UAU.4/PACE Single-use authentication mechanisms

FIA_UAU.4.1/PACE The TSF shall prevent reuse of authentication data related to **1.PACE Protocol according to** [R4]**,**

2.Authentication Mechanism based on Triple- DES and AES

3.Terminal Authentication Protocol v.1 according to [R5].

Application note:

The SFR FIA_UAU.4.1 in the current PP covers the definition in PACE PP [R16] and extends it 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 [R16].

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

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide **1. PACE Protocol according to** [R4]**,**

2. Passive Authentication according to [R6]

3. Secure messaging in MAC-ENC mode according to [R4]**,**

4. Symmetric Authentication Mechanism based on Triple-DES and AES

5. Terminal Authentication Protocol v.1 according to [R5]**,** to support user authentication.

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

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. The TOE accepts the authentication attempt as Personalisation Agent by [selection: the Authentication Mechanism with Personalisation Agent Key(s)].

3. After run of the Chip Authentication Protocol Version 1 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 v1.

4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 19.

5. [assignment: rules describing how the multiple authentication mechanisms provide authentication].

Application note:

The SFR FIA_UAU.5.1/PACE in the current PP covers the definition in PACE PP [R16] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in the current PP covers the definition in PACE PP [R16] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

FIA_UAU.6/EAC Re-authenticating

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 Version 1 shall be verified as being sent by the Inspection System**.

Application note:

The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [R6] 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 a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_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_API.1/CAP Authentication Proof of Identity

FIA_API.1.1/CAP The TSF shall provide a **Chip Authentication Protocol according to** [R5]to prove the identity of the **TOE**.

Application note:

This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [R5]. 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 [R6]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AAP Authentication Proof of Identity

FIA_API.1.1/AAP The TSF shall provide a **Active Authentication Protocol according to** [R6] to prove the identity of the **TOE**.

Application note:

This SFR has been added for the optional Active Authentication protocol. It requires the TOE to implement the Active Authentication Mechanism specified in [R6]. The terminal generates a secret then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corresponding to the Active Authentication public key (EF.DG14).

Class FDP User Data Protection

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

FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP** on **terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document**.

Application note:

The SFR FIA_ACC.1.1 in the current PP covers the definition in PACE PP [R16] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.

FDP_ACF.1/TRM Security attribute based access control

FDP_ACF.1.1/TRM The TSF shall enforce the **Access Control SFP** to objects based on the following: **1. Subjects:**

1.a. Terminal,

1.b. BIS-PACE

1.c. Extended Inspection System

2. Objects:

2.a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,

2.b. data in EF.DG3 of the logical travel document,

2.c. data in EF.DG4 of the logical travel document,

2.d. all TOE intrinsic secret cryptographic keys stored in the travel document

3. Security attributes:

3.a. PACE Authentication

3.b. Terminal Authentication v.1

3.c. Authorisation of the Terminal.

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** [R4] **after a successful PACE authentication as required by FIA_UAU.1/PACE**.

FDP_ACF.1.3/TRM The TSF shall explicitly authorise 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 following additional rules: **1. 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.

2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.

3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.

5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.

6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application note:

The SFR FDP_ACF.1.1/TRM in the current PP covers the definition in PACE PP [R16] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current PP cover the definition in PACE PP [R16]. The SFR FDP_ACF.1.4/TRM in the current PP covers the definition in PACE PP [R16] and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.

The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [R5]. 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.

Please note that the Document Security Object (SOD) stored in EF.SOD (see [R6]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [R4].

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).

Class FMT Security Management

The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

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

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles **1. Manufacturer,**

2. Personalisation Agent,

3. Terminal,

4. PACE authenticated BIS-PACE,

5. Country Verifying Certification Authority,

6. Document Verifier,

7. Domestic Extended Inspection System

8. Foreign Extended Inspection System.

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

Application note:

The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

The SFR FMT_SMR.1.1/PACE in the current PP covers the definition in PACE PP [R16] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

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

FMT_LIM.1 Limited capabilities

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 and disclosed,

2. TSF data to be disclosed or manipulated,

3. software to be reconstructed,

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

5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed

FMT_LIM.2 Limited availability

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 and disclosed,

2. TSF data to be disclosed or manipulated

3. software to be reconstructed,

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

5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,

Application note:

The formulation of 'Deploying Test Features' in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.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.

The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

FMT_MTD.1/CVCA_INI Management of TSF data

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,

4. [assignment: list of TSF data] to **Personalization Agent**.

Application note:

The ST writer shall perform the missing operation in the component FMT_MTD.1.1/CVCA_INI. The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalisation phase or by the Personalisation Agent (cf. [R5]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

FMT_MTD.1/CVCA_UPD Management of TSF data

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. [R5]). 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. [R5]).

FMT_MTD.1/DATE Management of TSF data

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. [R5]) 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 v.1 (cf. to [R5]).

FMT_MTD.1/CAPK Management of TSF data

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

Application note:

The component FMT_MTD.1/CAPK is refined by (i) selecting other operations and (ii) defining a selection for the operations 'create' and 'load' to be performed by the ST writer. The verb 'load' means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb 'create' means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1/CA as SFR for this key generation. The ST writer shall perform the assignment for the authorized identified roles in the SFR component FMT_MTD.1/CAPK.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the **1. PACE passwords,**

2. Chip Authentication Private Key,

3. Personalisation Agent Keys

4. Active Authentication Private Key to **none**.

Application note:

The SFR FMT_MTD.1/KEY_READ in the current PP covers the definition in PACE PP [R16] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for **TSF data of the Terminal Authentication Protocol v.1 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 Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE 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.

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 Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

FMT_MTD.1/AAPK Management of TSF data

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

Application note:

This SFR has been added for the optional Active Authentication protocol.

Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs 'Limited capabilities (FMT_LIM.1)', 'Limited availability (FMT_LIM.2)' together with the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions. The TOE shall meet the requirement 'TOE Emanation (FPT_EMS.1)' as specified below (Common Criteria Part 2 extended):

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **side channel** in excess of **limits of the state of the art** enabling access to **1. Chip Authentication Session Keys**

2. PACE session Keys (PACE-K MAC, PACE-KEnc),

3. the ephemeral private key ephem SK PICC-PACE,

4. Active Authentication Private Key,

5. Personalisation Agent Key(s),

6. Chip Authentication Private Key and **none**

FPT_EMS.1.2 The TSF shall ensure **any users** are unable to use the following interface **smart card circuit contacts** to gain access to **1. Chip Authentication Session Keys**

2. PACE Session Keys (PACE-K.MAC, PACE-K.Enc),

3. the ephemeral private key ephem SK PICC-PACE,

4. [assignment: list of types of TSF data],

5. Personalisation Agent Key(s) and

6. Chip Authentication Private Key and **none**.

Application note:

The SFR FPT_EMS.1.1 in the current PP covers the definition in PACE PP [R16] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in the current PP covers the definition in PACE PP [R16] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

The ST writer shall perform the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [R14] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). 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.

6.2 Security Assurance Requirements

The security assurance requirement level is EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Objectives

6.3.1.1 Security Objectives for the TOE

PP-0056

Security Objectives listed in PP PACE

OT.Data_Integrity The security objective **OT.Data_Integrity** 'Integrity of personal 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 FDP_UCT.1/TRM, 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_Confidentiality The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality 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.

OT.Tracing The security objective **OT.Tracing** 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:(i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) by FIA_AFL.1/PACE;(ii) for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) FTP_ITC.1/PACE.

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

OT.Prot_Inf_Leak The security objective **OT.Prot_Inf_Leak** 'Protection against Information Leakage' requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

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

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

OT.Identification The security objective **OT.Identification** 'Identification 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 cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Data_Authenticity The security objective **OT.Data_Authenticity** 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.AC_Pers The security objective **OT.AC_Pers** 'Access Control for Personalisation of logical travel document' 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-personalisation Data. 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 want 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.

Additional Security Objectives

OT.Sens_Data_Conf The security objective **OT.Sense_Data_Conf** 'Confidentiality of sensitive biometric reference data' is enforced by the Access Control SFP defined in FDP_ACC.1/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. 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.Chip_Auth_Proof 'Proof of travel document's chip authenticity' is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 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 [R5] 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.

6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Data_Integrity	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_MAC, FIA_UAU.6/PACE, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FPT_PHP.3, FCS_CKM.1/CA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/AAPK	Section 6.3.1
OT.Data_Confidentiality	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_ENC, FIA_UAU.6/PACE, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FCS_CKM.1/CA, FCS_COP.1/SYM, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ	Section 6.3.1
OT.Tracing	FIA_AFL.1/PACE, FTP_ITC.1/PACE	Section 6.3.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 6.3.1
OT.Prot_Inf_Leak	FPT_FLS.1, FPT_TST.1, FPT_PHP.3, FPT_EMS.1	Section 6.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 6.3.1
OT.Prot_Malfunction	FPT_FLS.1, FPT_TST.1	Section 6.3.1
OT.Identification	FMT_SMF.1, FMT_MTD.1/INI_ENA, FAU_SAS.1, FMT_SMR.1/PACE, FMT_MTD.1/INI_DIS	Section 6.3.1
OT.Data_Authenticity	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_MAC, FIA_UAU.6/PACE, FDP_RIP.1, FTP_ITC.1/PACE, FMT_SMF.1, FMT_MTD.1/PA, FCS_CKM.1/CA, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ	Section 6.3.1

OT.AC_Pers	FMT_SMF.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/PA, FAU_SAS.1, FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FPT_EMS.1, FMT_MTD.1/INI_DIS, FMT_LIM.1, FMT_LIM.2	Section 6.3.1
OT.Sens_Data_Conf	FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_UCT.1/TRM, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3, FMT_MTD.1/AAPK	Section 6.3.1
OT.Chip_Auth_Proof	FCS_CKM.1/CA, FCS_COP.1/SYM, FCS_COP.1/MAC, FMT_SMF.1, FMT_SMR.1/PACE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FIA_API.1/CAP, , FMT_MTD.1/AAPK, FIA_API.1/AAP, FCS_COP.1/SIG_GEN	Section 6.3.1

Table 7 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FCS_CKM.1/DH_PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity
FCS_CKM.4	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FCS_COP.1/PACE_ENC	OT.Data_Confidentiality
FCS_COP.1/PACE_MAC	OT.Data_Integrity, OT.Data_Authenticity
FIA_AFL.1/PACE	OT.Tracing
FIA_UAU.6/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity
FDP_RIP.1	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity
FDP_UCT.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.Sens_Data_Conf
FDP_UIT.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality
FTP_ITC.1/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Tracing, OT.Data_Authenticity
FMT_SMF.1	OT.Data_Integrity, OT.Data_Confidentiality, OT.Identification, OT.Data_Authenticity, OT.AC_Pers, OT.Chip_Auth_Proof
FMT_MTD.1/INI_ENA	OT.Identification, OT.AC_Pers
FMT_MTD.1/PA	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers
FPT_FLS.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_TST.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_PHP.3	OT.Data_Integrity, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper
FAU_SAS.1	OT.Identification, OT.AC_Pers

FCS_RND.1	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FMT_MTD.1/INI_DIS	OT.Identification, OT.AC_Pers
FCS_COP.1/SYM	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/SIG_VER	OT.AC_Pers, OT.Sens_Data_Conf
FCS_COP.1/MAC	OT.Data_Integrity, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/SIG_GEN	OT.Chip_Auth_Proof
FCS_CKM.1/CA	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FIA_UID.1/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FIA_UAU.1/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FIA_UAU.4/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FIA_UAU.5/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FIA_UAU.6/EAC	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf
FIA_API.1/CAP	OT.Chip_Auth_Proof
FIA_API.1/AAP	OT.Chip_Auth_Proof
FDP_ACC.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf

FDP_ACF.1/TRM	OT.Data_Integrity, OT.Data_Confidentiality, OT.AC_Pers, OT.Sens_Data_Conf
FMT_SMR.1/PACE	OT.Data_Integrity, OT.Data_Confidentiality, OT.Identification, OT.Data_Authenticity, OT.AC_Pers, OT.Chip_Auth_Proof
FMT_LIM.1	OT.Prot_Abuse-Func, OT.AC_Pers
FMT_LIM.2	OT.Prot_Abuse-Func, OT.AC_Pers
FMT_MTD.1/CVCA_INI	OT.Sens_Data_Conf
FMT_MTD.1/CVCA_UPD	OT.Sens_Data_Conf
FMT_MTD.1/DATE	OT.Sens_Data_Conf
FMT_MTD.1/CAPK	OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.1/KEY_READ	OT.Data_Integrity, OT.Data_Confidentiality, OT.Data_Authenticity, OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.3	OT.Sens_Data_Conf
FMT_MTD.1/AAPK	OT.Data_Integrity, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FPT_EMS.1	OT.Prot_Inf_Leak, OT.AC_Pers

Table 8 SFRs and Security Objectives

6.3.3 Dependencies

6.3.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/DH_PACE
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UAU.6/PACE	No dependencies	
FDP_RIP.1	No dependencies	
FDP_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/PACE, FDP_ACC.1/TRM
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/PACE, FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	
FMT_SMF.1	No dependencies	
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	
FAU_SAS.1	No dependencies	
FCS_RND.1	No dependencies	
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC
	(	
FIA_UID.1/PACE	No dependencies	

FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	
FIA_UAU.5/PACE	No dependencies	
FIA_UAU.6/EAC	No dependencies	
FIA_API.1/CAP	No dependencies	
FIA_API.1/AAP	No dependencies	
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FMT_MTD.1/CVCA_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
FMT_MTD.1/AAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FPT_EMS.1	No dependencies	
FCS_COP.1/SYM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/CA
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/CA
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/CA
FCS_COP.1/SIG_GEN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FCS_CKM.1/CA

Table 9 SFRs dependencies

<u>Rationale for the exclusion of dependencies</u>

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

6.3.3.2 SARs dependencies

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

Table 10 SARs dependencies

6.3.4 Rationale for the Security Assurance Requirements

The assurance level for this ST is EAL5+ augmented. The TOE is semiformally designed and tested. EAL5+ allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. The TOE is intended to operate in open environments, where attackers can easily exploit vulnerabilities. According to the usage of the TOE, it represents a significant value to perform attacks. In some malicious usages, of the TOE the statistical or probabilistic mechanisms in the TOE, for instance, may be subjected to analysis and attack in the normal course of operation. This level seems to be the reasonable minimum level for card hosting sensitive operations. The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's chip development and manufacturing especially for the secure handling of the MRTD's chip material. The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

The component ALC_DVS.2 has no dependencies. The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description,
- ADV_FSP.2 Security-enforcing functional specification,
- ADV_TDS.3 Basic modular design,
- ADV_IMP.1 Implementation representation of the TSF,
- AGD_OPE.1 Operational user guidance,
- AGD_PRE.1 Preparative procedures. All of these are met or exceeded in the EAL5+ assurance package.

6.3.4.1 AVA_VAN.5 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 and OT.Chip_Auth_Proof.

6.3.4.2 ALC_DVS.2 Sufficiency of security measures

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

7 TOE Summary Specification

7.1 TOE Summary Specification

7.1.1 Chip security functionalities

TSF_DPM

The chip identification data (O.Identification) is stored in a in the not changeable configuration page area and non-volatile memory. In the same area further TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During the production phase (phase 3 and 4) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to download, after a successful authentication process, a user specific encryption key and user code and data into the empty (erased) Infineon® SOLID FLASH memory area as specified by the associated control information of the Flash Loader software. The integrity of the loaded data is checked with a signature process. The data to be loaded may be transferred optionally in encrypted form. After finishing the load operation, the Flash Loader can be permanently deactivated, so that no further load operation with the Flash Loader is possible. During operation within a phase the accesses to memories are granted by the MMU controlled access rights and related privilege level. In addition, during each start-up of the TOE the address ranges and access rights are initialized by the STS with predefined values. During the testing phase in production within the secure environment the entire Infineon® SOLID FLASH is deleted.

TSF_PS

All contents of all memories of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. In addition the data transferred over the busses, the SFRs and the peripheral devices (CRC, RNG and Timer) are encrypted as well. The memory content and bus encryption is done by the MED using a complex key management and by the memories Infineon® SOLID FLASH, RAM, CACHE and the bus are entirely encrypted. Note that the FLASH contains the firmware only and no user data. Therefore, no data in plain are handled anywhere on the TOE and thus also the two CPUs compute entirely masked. The symmetric cryptographic co-processor is entirely masked as well. The user can define his own key for an Infineon® SOLID FLASH area to protect his data. This user individually chosen key is then delivered by the operating system and included in the dynamic Infineon® SOLID FLASH encryption. The user specified Infineon® SOLID FLASH area is then encrypted with his key and another component.

TSF_PMA

The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, FLASH and Infineon® SOLID FLASH and includes also the MED, MMU and the bus system. Thus introduced failures are detected and in certain errors are also automatically corrected. In order to prevent accidental bit faults during production in the FLASH, over the data stored in FLASH an EDC value is calculated. If a user tears the card resulting in a power off situation during an Infineon® SOLID FLASH programming operation or if other perturbation is applied, no data or content loss occurs and the TOE restarts power on.

TSF_PLA

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of the privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges, to a certain extend, for the privilege levels with the exception of the IFX level - is defined from the user software (OS).

TSF_CS

The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a co-processor supporting the DES and AES algorithms and a combination of a co-processor and software modules to support RSA cryptography, RSA key generation, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

7.1.2 Low level security functionalities

TSF_EXECUTION_ENVIRONMENT

This security functionality provides a secure execution environment based on the secure operation of CPU that controls the execution flow, detects and reacts to potential security violations. After start-up, this function calls TSF_BOOT_AT_POWER_UP and waits for a terminal command.

7.1.3 Operating system security functionalities

TSF_BOOT_AT_POWER_UP

This security functionality manages the initialization of the TOE that happens after each reset warm or cold. This security feature performs the following operations:

Test of the following items:

- FLASH memory segment
- RAM memory
- Random Number Generator
- Crypto-processor

- ATR issuing
- Initialization of all modules and applications initialization.

TSF_MEMORY_MANAGEMENT

This security functionality manages the persistent and volatile memories of the product according to the capacities of the underlying security IC, so as to control access to sensitive content protected by the TOE. TSF_MEMORY_MANAGEMENT manages the access to objects (files, directories, data and secrets) stored in FLASH. Access for read or write to RAM and FLASH is impossible from the outside, refer to TSF_IO_MANAGEMENT for more information.

Moreover, this security functionality uses TSF_CRYPTO_OPERATION to perform cryptographic operations in order to verify the integrity.

TSF_LIFE_CYCLE_MANAGEMENT

This security functionality manages the life cycle of the product and provides a secure transition mechanism between states. The various phases to be recognized are pre-personalization, personalization, usage and end of life. The management of the life cycle is performed by writing information in the One-Time Programmable (OTP) memory. The life cycle of the product is composed of 7 phases, more information is available in the dedicated paragraph 3.2 At the end of the fabrication phase, after a test phase, chip test mode is inhibited in a non-reversible way: the data (system or user) are completely under the control of the card operating system. This is true for read, write or modify operations. Tests done during fabrication phase can not be used anymore.

TSF_CPLC

This security functionality manages the CPLC area. The CPLC area contains Manufacturing data, pre-personalization data and Personalization data. Manufacturing data are written by the Manufacturer during the Manufacturing phase and contain identification data such as founder ID, chip ID and operating system ID. Pre-Personalization data are written by the Manufacturer and also contains identification data such as the module ID. The CPLC area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Read access to the CPLC area is allowed during Personalization phase. During Operational Use phase, the CPLC area read access is only possible after PACE authentication.

TSF_MONITORING

This Security Functionality monitors all the events generated by the security IC physical detectors:

- Bad CPU usage
- integrity loss in FLASH, OTP or RAM,

- code signature alarm,
- fault injection attempt,
- watchdog timeout,
- access attempt to unavailable or reserved memory areas,
- MPU errors,
- clock and voltage supply operating changes by the environment,
- TOE physical integrity abuse.

Executable code integrity is controlled during its execution through the addition of code redundancies and specific tests. Code consistency is then ensured.

TSF_IO_MANAGEMENT

This security functionality manages Input/Output interfaces by way of contact and contactless. Two protocols are used to communicate:

- T=0 protocol, asynchronous, character-oriented half-duplex transmission protocol
- T=CL, specific to the contactless, asynchronous, block-oriented half-duplex transmission protocol

A buffer is used for inputs and outputs. It is a reserved memory zone for the communication. Other memories can not be accessed. During a cryp- tographic operation, the access to this buffer is blocked, once the operation is finished, the integrity of the buffer is verified by a CRC.

TSF_ALEA

This security functionality provides random numbers. The random number generation is in conformance to the quality requirements of the french national schemes:

- A random number generator compliant with the French Scheme ANSSI requirements for RNG
- A random generator of n bytes.

The chip security functionality is compliant with the AIS31 standard. Conforming to the French Scheme ANSSI requirement for RNG, post-treatment is effectued on the RNG chip output, directly by the chip. The RNG chip output provided by the chip s submitted to a posttreatment in order to provide a random number of n bytes.

7.1.4 Application security functionalities

TSF_KEY_MANAGEMENT

This security functionality provides secure generation, destruction, replacement and storage of cryptographic keys (KEY, PIN) according to the specification of the product. Each secret is identified by a unique identifier and only manipulated with the help of this identifier by the cryptographic module.

Each secret is associated to a ratification counter. The management of these lasts is made by read/write control of the management of the maximum number of attempts.

TSF_PACE_AUTH

This security functionality manages the authentication of the Inspection system to the TOE, based on the Document Basic Access Keys. TSF_PACE_AUTH performs the Password Authenticated Connection Establishment mechanism, as described in [R5], in order to authenticate the Inspection System. TSF_PACE_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

TSF_CRYPTO_OPERATION

This security functionality performs high level cryptographic operations:

Encryption/decryption;

Integrity verification;

Secret decryption;

Authentication cryptogram creation/verification;

Key derivation;

Hash value calculation.

TSF_TERM_AUTH

This security function manages the authentication of the Terminal to the TOE, based on the authentication secrets related to the Terminal. TSF_TERM_AUTH performs the Terminal Authentication to authenticate the terminal. TSF_TERM_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

TSF_SYM_AUTH

This security function manages the authentication of a user to the TOE, based on the TDES or AES keys related to this user, during the personalization phase. TSF_SYM_AUTH performs an authentication mechanism based on TDES or AES. TSF_SYM_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

TSF_CHIP_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Chip Authentication Protocol as defined in [R5]. TSF_CHIP_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations

TSF_ACTIVE_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Active Authentication Protocol as defined in [R5]. TSF_ACTIVE_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations

7.2 SFRs and TSS

7.2.1 SFRs and TSS - Rationale

7.2.1.1 Security Functional Requirements

PP-0056

SFRs listed in PP PACE

FCS_CKM.1/DH_PACE is met by TSF_PACE_AUTH and TSF_CRYPTO_OPERATION, which performs, as described in [R5], sec. 3.1 and Annex A.1:

the Diffie-Hellman Protocol compliant with PKCS#3 to generate session keys of size 1024, 1536 and 2048 bits,

the ECDH compliant to ISO 159464

[R17] to generate session keys of size 192, 224 and 256 bits. FCS_CKM.1/DH_ MRTD is also met by TSF_KEY_MANAGEMENT, which ensures the protection of the keys during generation.

FCS_CKM.4 is met by TSF_KEY_MANAGEMENT and by TSF_MEMORY_MANAGEMENT, as TSF_KEY_MANAGEMENT manages the secure destruction of secret by calling TSF_MEMORY_MANAGEMENT.

FCS_COP.1/PACE_ENC is met by TSF_CS, TSF_CRYPTO_OPERATION, which performs TDES encryption and decryption, in conformance with FIPS 46-3 normative appendix 5, A5.3, in order to achieve secure messaging - confidentiality.

FCS_COP.1/PACE_MAC is met by TSF_CS, TSF_CRYPTO_OPERATION, which performs TDES encryption and decryption, in conformance with FIPS 46-3 normative appendix 5, A5.3, in order to achieve secure messaging - confidentiality.

FIA_AFL.1/PACE is met by TSF_KEY_MANAGEMENT, which ensures, when a counter is related to an authentication key, that the counter is incremented in case of authentication failure, that the counter is reinitialized in case of authentication success and that the authentication key is blocked in case of 32 successive authentication attempts.

FIA_UAU.6/PACE is met by TSF_CRYPTO_OPERATION, which provide the re-authentication mechanism by means of the secure messaging, and by

TSF_EXECUTION_ENVIRONMENT which ensures that only commands consistent with the security state of the card are accepted.

FDP_RIP.1 is met by TSF_KEY_MANAGEMENT and TSF_MEMORY_MANAGEMENT, which ensures allocation and desallocation of memory for secret keys.

FDP_UCT.1/TRM is met by TSF_CHIP_AUTH and TSF_CRYPTO_OPERATION, which ensures that a secure messaging in integrity and confidentiality is established after Chip Authentication, therefore enabling to protect transmitted and received data from disclosure and by TSF_EXECUTION_ENVIRONMENT, which verifies the security status of the received command, and will therefore detect if secure messaging is interrupted.

FDP_UIT.1/TRM is met by TSF_CHIP_AUTH and TSF_CRYPTO_OPERATION, which ensures that a secure messaging in integrity and confidentiality is established after Chip Authentication, therefore enabling to protect transmitted and received data from modification and by TSF_EXECUTION_ENVIRONMENT, which verifies the security status of the received command, and will therefore detects if secure messaging is interrupted.

FTP_ITC.1/PACE is met by TSF_PACE_AUTH, TSF_TERM_AUTH which manages the authentication of the Terminal to the TOE, based on the authentication secrets related to the Terminal. TSF_TERM_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

FMT_SMF.1 is met by TSF_LIFE_CYCLE_MANAGEMENT, which manages a life cycle that includes a pre-personalization (initialization) and a personalization phase, and by TSF_EXECUTION_ENVIRONMENT, which ensures that only the AIP application is selectable in pre-personalization (initialization) and personalization phases.

FMT_MTD.1/INI_ENA is met by TSF_IO_MANAGEMENT, which manages the area where the initialization and pre-personalization data are written.

FMT_MTD.1/PA is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, and by TSF_SYM_AUTH, which ensures that the personalization Agent is authenticated.

FPT_FLS.1 is met by TSF_DPM and TSF_MONITORING which ensure that a secure state of the TOE (whether by reset or card termination) is maintained whenever a default or an anomaly is detected. FPT_FLS.1 is also met by

TSF_EXECUTION_ENVIRONMENT which ensures the detection of a tampering attempt, of a default or of an anomaly.

FPT_TST.1 is met by TSF_BOOT_AT_POWER_UP which automatically performs testing of critical elements of the TOE at power-up. FPT_TST.1 is also met by TSF_EXECUTION_ENVIRONMENT which tests the integrity of accessed objects.

FPT_PHP.3 is met by TSF_EXECUTION_ENVIRONMENT, TSF_MONITORING, TSF_DPM and TSF_PMA which monitor the TOE and react when a security event is detected, therefore protecting the TOE from probing or physical manipulation.

FAU_SAS.1 is met by TSF_LIFE_CYCLE_MANAGEMENT, which manages the write-only-once OTP area where TOE parameters, such as the life phase, are written, and by TSF_CPLC, which manages the write-only-once CPLC area where TOE identification data are written.

FCS_RND.1 is met by TSF_ALEAS, which generates random numbers using a random number generator that complies with the AIS31 Class P2 quality metric.

FMT_MTD.1/INI_DIS is met by TSF_CPLC, which manages the area where the initialization and pre-personalization data are written.

Additional SFRs

Class Cryptographic Support (FCS) Cryptographic operation (FCS_COP.1)

FCS_COP.1/SYM is met by TSF_CS, TSF_CRYPTO_OPERATION, which performs TDES encryption and decryption, in conformance with FIPS 46-3 normative appendix 5, A5.3, in order to achieve secure messaging - confidentiality.

FCS_COP.1/SIG_VER is met by TSF_CS, TSF_CRYPTO_OPERATION, which performs signature verification.

FCS_COP.1/MAC is met by TSF_CS, TSF_CRYPTO_OPERATION, which performs Retail MAC in conformance with ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) in order to achieve secure messaging - integrity.

FCS_COP.1/SIG_GEN is met by TSF_CRYPTO_OPERATION and TSF_CS, which performs: RSA with keys of size 1024, 1536, 2048 and 3072 bits in conformance with ISO9796-2 Digital Signature scheme 1, in order to achieve digital signature generation, as required by FCS_COP.1/SIG_GEN.

Miscellaneous

FCS_CKM.1/CA is met by TSF_CRYPTO_OPERATION, which performs normative appendix 5 Document Basic Access Key Derivation Algorithm to generate session keys of 112 bits. FCS_CKM.1 is also met by TSF_KEY_MANAGEMENT, which ensures the protection of the keys during generation.

FIA_UID.1/PACE is met by TSF_PACE_AUTH, TSF_LIFE_CYCLE_MANAGEMENT and TSF_BOOT_AT_POWER_UP, which manage the initialization of the communication with the card and manages the card life cycle, and TSF_CPLC, which manages the CPLC area where the initialization and pre-personalization data are stored.

FIA_UAU.1/PACE is met by **TSF_PACE_AUTH**, TSF_LIFE_CYCLE_MANAGEMENT and TSF_BOOT_AT_POWER_UP, which manage the initialization of the communication with the card, and manage the OTP area where the current phase of the TOE is stored, by TSF_CPLC, which manages the area where the initialization and pre-personalization data are stored and by TSF_TERM_AUTH and TSF_SYM_AUTH which manage user authentication (and thus key selection).

FIA_UAU.4/PACE is met **TSF_PACE_AUTH** ,TSF_TERM_AUTH and TSF_SYM_AUTH, TSF_CRYPTO_OPERATION and TSF_ALEA which ensure that each authentication of a user is performed using a random challenge, which prevents reuse of the authentication data.

FIA_UAU.5/PACE is met by **TSF_PACE_AUTH** ,TSF_TERM_AUTH, TSF_SYM_AUTH and TSF_CRYPTO_OPERATION, which support all the authentication mechanisms required by FIA_UAU.5, and by TSF_EXECUTION_ENVIRONMENT which ensures that only commands consistent with the security state of the card are accepted.

FIA_UAU.6/EAC is met by TSF_CRYPTO_OPERATION which provide the re-authentication mechanism by means of the secure messaging, and by TSF_EXECUTION_ENVIRONMENT which ensures that only commands consistent with the security state of the card are accepted.

FIA_API.1/CAP is met by TSF_CHIP_AUTH which supports TOE authentication to the terminal using the Chip Authentication Protocol as defined in[R5]. FIA_API.1/CAP is met by TSF_CRYPTO_OPERATION which supports the SFR by providing cryptographic features.

FIA_API.1/AAP is met by TSF_ACTIVE_AUTH, which supports TOE authentication to the terminal using the Active Authentication Protocol as defined in[R6]. FIA_API.1/AAP is met by TSF_CRYPTO_OPERATION which supports the SFR by providing cryptographic features.

Class FDP User Data Protection

FDP_ACC.1/TRM is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication or secure messaging, are fulfilled before authorizing access to an object, and by TSF_EXECUTION_ENVIRONMENT which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/TRM is met by TSF_PLA and TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication or secure messaging, are fulfilled before authorizing access to an object, and by TSF_EXECUTION_ENVIRONMENT which verify that each received command security status is consistent with the security status of the TOE.

Class FMT Security Management

FMT_SMR.1/PACE is met by TSF_PACE_AUTH, TSF_TERM_AUTH and TSF_SYM_AUTH, which provide user authentication mechanism and by TSF_KEY_MANAGEMENT which manages the identification number of the secret, therefore allowing the TOE to maintain different user roles.

FMT_LIM.1 is met by TSF_PS, TSF_EXECUTION_ENVIRONMENT and TSF_BOOT_AT_POWER_UP as those security functions provide test features of the TOE after TOE delivery, which do not allow disclosure or unauthorized manipulation of TSF data, user data, software or any other substantial information.

FMT_LIM.2 is met by TSF_PS, TSF_EXECUTION_ENVIRONMENT and TSF_BOOT_AT_POWER_UP as those security functions provide test features of the TOE after TOE delivery, which do not allow disclosure or unauthorized manipulation of TSF data, user data, software or any other substantial information.

FMT_MTD.1/CVCA_INI is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, and by TSF_SYM_AUTH which ensures that the Personalization Agent is authenticated.

FMT_MTD.1/CVCA_UPD is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, and by TSF_TERM_AUTH which ensures that the Country Verifier Certification Authority is authenticated.

FMT_MTD.1/DATE is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, by TSF_TERM_AUTH which ensures that the Country Verifier Certification Authority is authenticated, which ensures that the Document Verifier is authenticated, and which ensures that the Domestic Extended Inspection System is authenticated.

FMT_MTD.1/CAPK is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, and by TSF_SYM_AUTH which ensures that the Personalization Agent is authenticated.

FMT_MTD.1/KEY_READ is met by TSF_IO_MANAGEMENT which ensures that all the access conditions to an object, such as never for instance, are respected. FMT_MTD.1/KEY_READ is also supported by TSF_KEY_MANAGEMENT which ensures that operations on secret keys does not allow any read access to those keys.

FMT_MTD.3 is met by TSF_CRYPTO_OPERATION which performs signature verification and therefore verifies the correctness of the digital signature of the certificates involved in a terminal authentication.

FMT_MTD.1/AAPK is met by TSF_IO_MANAGEMENT which ensures that all the access conditions, such as user authentication, are fulfilled before authorizing access to an object, and by TSF_SYM_AUTH which ensures that the Personalization Agent is authenticated.

Class FPT Protection of the Security Functions

FPT_EMS.1 is met by TSF_PMA, TSF_EXECUTION_ENVIRONMENT which provides interruption in order to avoid information leakage trough observation of emanation. FPT_EMS.1 is also met by TSF_CRYPTO_OPERATION and TSF_KEY_MANAGEMENT which ensure secure execution of cryptographic operations on keys such as the Personalization Agent Authentication Key.

7.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FCS_CKM.1/DH_PACE	TSF_KEY_MANAGEMENT, TSF_CRYPTO_OPERATION, TSF_PACE_AUTH
FCS_CKM.4	TSF_MEMORY_MANAGEMENT, TSF_KEY_MANAGEMENT
FCS_COP.1/PACE_ENC	TSF_CRYPTO_OPERATION, TSF_CS
FCS_COP.1/PACE_MAC	TSF_CRYPTO_OPERATION, TSF_CS
FIA_AFL.1/PACE	TSF_KEY_MANAGEMENT
FIA_UAU.6/PACE	TSF_CRYPTO_OPERATION, TSF_EXECUTION_ENVIRONMENT
FDP_RIP.1	TSF_KEY_MANAGEMENT, TSF_MEMORY_MANAGEMENT
FDP_UCT.1/TRM	TSF_CRYPTO_OPERATION, TSF_CHIP_AUTH, TSF_EXECUTION_ENVIRONMENT
FDP_UIT.1/TRM	TSF_CRYPTO_OPERATION, TSF_CHIP_AUTH, TSF_EXECUTION_ENVIRONMENT
FTP_ITC.1/PACE	TSF_CRYPTO_OPERATION, TSF_TERM_AUTH, TSF_PACE_AUTH
FMT_SMF.1	TSF_LIFE_CYCLE_MANAGEMENT, TSF_EXECUTION_ENVIRONMENT
FMT_MTD.1/INI_ENA	TSF_IO_MANAGEMENT
FMT_MTD.1/PA	TSF_IO_MANAGEMENT, TSF_SYM_AUTH
FPT_FLS.1	TSF_MONITORING, TSF_DPM, TSF_EXECUTION_ENVIRONMENT
FPT_TST.1	TSF_EXECUTION_ENVIRONMENT, TSF_BOOT_AT_POWER_UP
FPT_PHP.3	TSF_EXECUTION_ENVIRONMENT, TSF_MONITORING, TSF_PMA, TSF_DPM
FAU_SAS.1	TSF_LIFE_CYCLE_MANAGEMENT, TSF_CPLC
FCS_RND.1	TSF_ALEA
FMT_MTD.1/INI_DIS	TSF_CPLC
FCS_COP.1/SYM	TSF_CRYPTO_OPERATION, TSF_CS
FCS_COP.1/SIG_VER	TSF_CRYPTO_OPERATION, TSF_CS
FCS_COP.1/MAC	TSF_CRYPTO_OPERATION, TSF_CS
FCS_COP.1/SIG_GEN	TSF_CRYPTO_OPERATION, TSF_CS
FCS_CKM.1/CA	TSF_KEY_MANAGEMENT, TSF_CRYPTO_OPERATION
FIA_UID.1/PACE	TSF_LIFE_CYCLE_MANAGEMENT, TSF_CPLC, TSF_BOOT_AT_POWER_UP, TSF_PACE_AUTH
FIA_UAU.1/PACE	TSF_LIFE_CYCLE_MANAGEMENT, TSF_CPLC, TSF_TERM_AUTH, TSF_PACE_AUTH,TSF_SYM_AUTH, TSF_BOOT_AT_POWER_UP

FIA_UAU.4/PACE	TSF_CRYPTO_OPERATION, TSF_TERM_AUTH, TSF_SYM_AUTH, TSF_ALEA, TSF_PACE_AUTH
FIA_UAU.5/PACE	TSF_CRYPTO_OPERATION, TSF_TERM_AUTH, TSF_SYM_AUTH, TSF_EXECUTION_ENVIRONMENT, TSF_PACE_AUTH
FIA_UAU.6/EAC	TSF_CRYPTO_OPERATION, TSF_EXECUTION_ENVIRONMENT
FIA_API.1/CAP	TSF_CRYPTO_OPERATION, TSF_CHIP_AUTH, TSF_ACTIVE_AUTH
FIA_API.1/AAP	TSF_CRYPTO_OPERATION, TSF_CHIP_AUTH, TSF_ACTIVE_AUTH
FDP_ACC.1/TRM	TSF_IO_MANAGEMENT, TSF_EXECUTION_ENVIRONMENT
FDP_ACF.1/TRM	TSF_IO_MANAGEMENT, TSF_EXECUTION_ENVIRONMENT, TSF_PLA
FMT_SMR.1/PACE	TSF_KEY_MANAGEMENT, TSF_TERM_AUTH, TSF_SYM_AUTH, TSF_PACE_AUTH
FMT_LIM.1	TSF_PS, TSF_EXECUTION_ENVIRONMENT, TSF_BOOT_AT_POWER_UP
FMT_LIM.2	TSF_PS, TSF_EXECUTION_ENVIRONMENT, TSF_BOOT_AT_POWER_UP
FMT_MTD.1/CVCA_INI	TSF_IO_MANAGEMENT, TSF_SYM_AUTH
FMT_MTD.1/CVCA_UPD	TSF_IO_MANAGEMENT, TSF_TERM_AUTH
FMT_MTD.1/DATE	TSF_IO_MANAGEMENT, TSF_TERM_AUTH
FMT_MTD.1/CAPK	TSF_IO_MANAGEMENT, TSF_SYM_AUTH
FMT_MTD.1/KEY_READ	TSF_IO_MANAGEMENT, TSF_KEY_MANAGEMENT
FMT_MTD.3	TSF_CRYPTO_OPERATION
FMT_MTD.1/AAPK	TSF_IO_MANAGEMENT, TSF_SYM_AUTH
FPT_EMS.1	TSF_EXECUTION_ENVIRONMENT, TSF_KEY_MANAGEMENT, TSF_CRYPTO_OPERATION, TSF_PMA

Table 11 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
TSF_DPM	FPT_FLS.1, FPT_PHP.3
TSF_PS	FMT_LIM.1, FMT_LIM.2
TSF_PMA	FPT_PHP.3, FPT_EMS.1
TSF_PLA	FDP_ACF.1/TRM
TSF_CS	FCS_COP.1/SYM, FCS_COP.1/SIG_VER, FCS_COP.1/MAC, FCS_COP.1/SIG_GEN, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC
TSF_EXECUTION_ENVIRONMENT	FPT_PHP.3, FPT_EMS.1, FIA_UAU.6/PACE, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FMT_SMF.1, FPT_FLS.1, FPT_TST.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_LIM.1, FMT_LIM.2
TSF_BOOT_AT_POWER_UP	FIA_UID.1/PACE, FIA_UAU.1/PACE, FPT_TST.1, FMT_LIM.1, FMT_LIM.2
TSF_MEMORY_MANAGEMENT	FCS_CKM.4, FDP_RIP.1
TSF_LIFE_CYCLE_MANAGEMENT	FMT_SMF.1, FAU_SAS.1, FIA_UID.1/PACE, FIA_UAU.1/PACE
TSF_CPLC	FAU_SAS.1, FMT_MTD.1/INI_DIS, FIA_UID.1/PACE, FIA_UAU.1/PACE
TSF_MONITORING	FPT_FLS.1, FPT_PHP.3
TSF_IO_MANAGEMENT	FMT_MTD.1/INI_ENA, FMT_MTD.1/PA, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.1/AAPK
TSF_ALEA	FCS_RND.1, FIA_UAU.4/PACE
TSF_KEY_MANAGEMENT	FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_CKM.1/CA, FMT_SMR.1/PACE, FMT_MTD.1/KEY_READ, FPT_EMS.1, FIA_AFL.1/PACE, FDP_RIP.1
TSF_CRYPTO_OPERATION	FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE, FCS_CKM.1/CA, , FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/EAC, FIA_API.1/CAP, FIA_API.1/AAP, FMT_MTD.3, FPT_EMS.1, FCS_COP.1/SYM, FCS_COP.1/SIG_VER, FCS_COP.1/MAC, FCS_COP.1/SIG_GEN, FIA_UAU.6/PACE

TSF_TERM_AUTH	FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FMT_SMR.1/PACE, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FTP_ITC.1/PACE
TSF_SYM_AUTH	FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FMT_SMR.1/PACE, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CAPK, FMT_MTD.1/AAPK, FMT_MTD.1/PA
TSF_CHIP_AUTH	FDP_UCT.1/TRM, FDP_UIT.1/TRM, FIA_API.1/CAP, FIA_API.1/AAP
TSF_ACTIVE_AUTH	FIA_API.1/CAP, FIA_API.1/AAP
TSF_PACE_AUTH	FCS_CKM.1/DH_PACE, FIA_UID.1/PACE, FTP_ITC.1/PACE, FIA_UAU.1/PACE FIA_UAU.4/PACE, FIA_UAU.5/PACE, FMT_SMR.1/PACE

Table 12 TSS and SFRs - Coverage

8 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

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

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

All subjects and objects addressed by more than one SFR are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items.

The assurance class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise. Furthermore, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

9 Security Attributes, Keys and Certificates

Security attributes

Security attributes	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [R5]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [R5]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [R5]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [R5]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [R5])
	DG3 (Fingerprint)	Read access to DG3: (cf. [R5])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [R5])

Keys and Certificates

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [R7].

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK.CVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SK.CVCA) used for signing the Document Verifier Certificates.
Country Verifying	The TOE stores the Country Verifying Certification Authority
Certification Authority Public Key (PK.CVCA)	Public Key (PK.CVCA) as part of the TSF data to verify the Document Verifier Certificates. The PK.CVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C.CVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [R5] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK.CVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C.DV)	The Document Verifier Certificate C.DV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK.DV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C.IS)	The Inspection System Certificate (C.IS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK.IS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.

Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK.ICC, PK.ICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [R11].
Chip Authentication Public Key (PK.ICC)	The Chip Authentication Public Key (PK.ICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK.ICC)	The Chip Authentication Private Key (SK.ICC) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organisation 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 Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organisation with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

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 travel document's point of view the domestic Document Verifier belongs to the issuing State or Organisation.

10 Statement of compatibility

The statement of compatibility address the specific requirements for composite evaluation as stated in the document "Composite product evaluation for Smartcards and similar devices" [R12]. The rational explaining how these specific requirements are addressed is presented in the same logical order than the work item stated in [R12].

10.1 Separation of the Platform-TSF

This section describes the separation of relevant security functionality described in the ST of the Infineon Technologies M7892 B11 platform with specific IC dedicated software and optional RSAv1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries being used by this ST. The security functionality provided by the IC platform is summarized in [R8], chapter 8. The following table lists the relevant security functionality of the platform regarding cryptography with regards to those of the composite TOE defined in the present ST.

Platform functionality	Usage by the composite TOE
Device Phase Management	This functionality is automatically triggered at start'up. The composite TOE takes over with its functionality TSF_CPLC.
Protection against Logical Attacks	This functionality is directly identified by the composite TOE through its security functionalities TSF_ACTIVE_AUTH, TSF_SYM_AUTH, TSF_TERM_AUTH, TSF_PACE_AUTH, TSF_CHIP_AUTH
Protection against Snooping	This functionality is used by the composite TOE functionality TSF_KEY_MANAGEMENT, as a hardware underlying mechanism.
Protection against Modifying Attacks	This functionality is directly identified by the composite TOE through its functionalities TSF_EXECUTION_ENVIRONMENT and TSF_MONITORING
Cryptographic Support	The TDES functionality is directly identified by the composite TOE through its functionality TSF_CS which is used by TSF_CRYPTO_OPERATION. The SHA functionality is directly identified by the composite TOE through its functionality TSF_CS which is used by TSF_CRYPTO_OPERATION. The TRNG functionality is directly identified by the composite TOE through its functionality TSF_CS and used by TSF_CRYPTO_OPERATION. The AES functionality is not used. RSA and Elliptic Curve functionalities are not used.

Table 13: Coverage of IC platform functionality

In the following table the SFRs of the IC platform are designated as "relevant" or "used by this composite ST". The table also lists explicitly irrelevant Platform-SFRs not being used by the Composite-ST.

Platform SFRs	Usage by TOE, TOE-SFR
FRU_FLT.2	Internal IC mechanism. Supporting TSF_PMA
FPT_FLS.1	TSF_PS, TSF_PMA, TSF_PLA, TSF_CS
FMT_LIM.1	TSF_DPM
FMT_LIM.2	TSF_DPM
FAU_SAS.1	TSF_DPM, , TSF_CPLC ,FAU_SAS.1
FPT_PHP.3	TSF_DPM, TSF_PS, TSF_PMA, TSF_PLA, TSF_CS, TSF_PHY / FPT_PHP.3
FDP_ITT.1	Internal IC mechanism. Supporting TSF_DPM, TSF_PS, TSF_PMA, TSF_PLA, TSF_CS, TSF_CRYPTO_OPERATION
FPT_ITT.1	Internal IC mechanism. Supporting TSF_DPM, TSF_PS, TSF_PMA, TSF_CRYPTO_OPERATION
FDP_IFC.1	Internal IC mechanism. Supporting TSF_PS, TSF_PMA, TSF_PLA, TSF_CRYPTO_OPERATION
FCS_RNG.1	TSF_ALEAS / FCS_RND.1
FPT_TST.2	TSF_PMA, TSF_CS
FDP_ACC.1	TSF_DPM, TSF_PMA, TSF_PLA, FDP_ACC.1
FDP_ACF.1	TSF_DPM, TSF_PMA, TSF_PLA, FDP_ACF.1
FMT_SMF.1	TSF_DPM, TSF_PMA, TSF_PLA,, FMT_SMF.1
FCS_COP.1	TSF_CS
FCS_CKM.1	Irrelevant. Unused for TOE SFRs
FDP_SDI.1	TSF_PMA
FDP_SDI.2	TSF_PMA
FMT_MSA.3	Irrelevant. Unused for TOE SFRs.
FMT_MSA.1	Irrelevant. Unused for TOE SFRs.

Table 14: Coverage of IC platform SFRs

10.2 Statement of compatibility for the security assurance requirements

This statement of compatibility address the requirement specified in [R12] for the security assurance requirements.

The security requirement for the underlying IC M7892 B11 specified in its security target [R8] is EAL6 augmented with the following component: ALC_FLR.1 where the security assurance requirement for the composite TOE is EAL5+ augmented with the following component: ALC_DVS.2 and AVA_VAN.5

Therefore, the security assurance requirements for the composite TOE represent a subset of the security assurance requirements of the underlying platform.

10.3 Statement of compatibility for the security environment and the objectives

10.3.1 Objectives

There is no conflict between security objectives of the Composite Security Target and the IC Security Target. All IC platform objectives are relevant, even if some of them are partially used (O.Add-Functions and O.Mem-Access).

Objectives for the IC	Objectives for the composite TOE	Remarks
O.Leak-Inherent	OT.Prot_Inf_Leak	Objective covering also O.Leak-Forced
O.Phys-Probing	OT.Prot_Phys-Tamper	Objective covering also O.Phys-Manipulation
O.Malfunction	OT.Prot_Malfunction	Full coverage
O.Phys-Manipulation	OT.Prot_Phys-Tamper	Objective covering also O.Phys-Probing
O.Leak-Forced	OT.Prot_Inf_Leak	Objective covering also O.Leak-Inherent
O.Abuse-Func	OT.Prot_Abuse-Func	Full coverage
O.Identification	OT.Identification	Full coverage
O.RND	No equivalent as the final composite TOE does not aim to offer random number generation, but to use the one offered by the IC	
O.Add-Functions	No equivalent as the final composite TOE does not aim to offer cryptographic services, but to use the ones offered by the IC	O.Add-Functions contributes to : OT_Sens_Data_Conf
O.Mem Access	No equivalent as the final composite TOE uses the hardware functionality for a final purpose : enforce the Extended Access Control specified through : OT.Sens_Data_Conf.	O.Mem-Access contributes to OT.Sens_Data_Conf and OT.AC_Pers
OE.Plat-Appl		Covered through ADV. Not an objective on the operational environment
OE.Resp-Appl		Covered through ADV/ALC/ATE/AVA. Not an objective on the operational environment
OE.Process-Sec-IC		Covered through ADV/ALC/ATE/AVA. Not an objective on the operational environment

Table 15: Coverage of IC platform objectives

Note that all additional objectives on the environment for the composite TOE are for the operational environment, and do not contradict the IC objectives.

10.3.2 Threats

There is no conflict between threats of the Composite Security Target and the IC Security Target.

Threats for the IC	Threats for the composite TOE	Remarks
T.Leak-Inherent	T.Information_Leakage	Threats also including T.Read_Sensitive_Data
T.Phys-Probing	T.Phys-Tamper	
T.Malfunction	T.Malfunction	Full match
T.Phys-Manipulation	T.Phys-Tamper	
T.Leak-Forced	T.Information_Leakage	Threats also including T.Read_Sensitive_Data
T.Abuse-Func	T.Abuse-Func	Full match
T.RND	No equivalent as this threats is already covered by the IC internal mechanism (O.RND and FCS_RNG.1)	
T.Mem-Access	T.Skimming, T.Forgery	The two identified threats for the composite TOE address a more specific risk, however, the main principle remain the same.

Table 16: Coverage of threats

10.3.3 Organisational security policies

There is no conflict between OSPs of the Composite Security Target and the IC Security Target.

OSPs for the IC	OSPs for the composite TOE	Remarks
P.Process-TOE	No equivalent but this OSP covers the development and manufacturing environment (covered by ALC class)	
P.Add-Functions	As for O.Add-Functions, there is no equivalent as the final composite TOE does not aim to offer cryptographic services, but to use the ones offered by the IC	contributes to : OT.Sens_Data_Conf

Table 17: Coverage of OSPs

The P.Add-functions introduces the IC cryptographic services to be used by the embedded software. There is no contradiction with the threats or objectives for the composite TOE.

10.3.4 Assumptions

There is no conflict between assumption of the Composite Security Target and the IC Security Target.

Assumption for the IC	Assumptions/Objectives/SAR for the composite TOE	Remarks
A.Process-Sec-IC	Covered through ALC/ADV	
A.Plat-Appl	Covered through assurance class ADV. Not an assumption on the operational environment	assumptions not significant for the composite TOE
A.Resp-Appl	Covered through assurance class ADV/ALC/ATE/AVA. Not an assumption on the operational environment	assumptions not significant for the composite TOE
A.Key-Function	OT.Prot_inf_leak	

Table 18: Coverage of assumptions

There is only one significant assumption for the composite TOE that is fully addressed by the current composite security target.

Note that all additional assumptions for the composite TOE are for the operational environment, and do not contradict the IC threats.

11 Glossary and Acronyms

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [R5].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [R4], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO.D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [R6] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
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 travel document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organisation
Basic Access Control (BAC)	Security mechanism defined in [R6] by which means the travel document'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 with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographic data (biodata).	The personalised details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [R6]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [R6]

Country Signing CA Certificate (C.CSCA)	Certificate of the Country Signing Certification Authority Public Key (K.PuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [R6], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [R6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [R5].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [R5]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [R6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [R5].
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.

CV Certificate	Card Verifiable Certificate according to [R5].
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 [R6] 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.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [R4],
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO.D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (C.DS). [R6]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [R5]and [R6]. This role is usually delegated to a Personalisation Agent.

Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [R5]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this PP. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document'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. [R6]
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [R5].

Extended Access Control	Security mechanism identified in [R6] by which means the travel document'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.
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 Organisation 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. [R6]
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 travel documents. [R6]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
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 Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [R6]
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. [R6]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
Initialisation 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 travel document's material (IC identification data).
Inspection	The act of a State examining an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [R6]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organisation

Issuing Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [R6]
Issuing State	The Country issuing the travel document. [R6]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [R6]. The capacity expansion technology used is the travel document's chip.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [R6] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1. personal data of the travel document holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [R6]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [R6] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
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. [R6]

Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [R5]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
ePassport application	Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes ● **the file structure implementing the LDS** [R6], ● 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.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [R4],. 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.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [R5], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [R6] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.

Personalisation Data	A set of data incl. (i)individual-related data (biographic and biometric data) of the travel document holder, (ii)dedicated document details data and (iii)dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalisation Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair.
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the traveller is applying for entry. [R6]
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.

RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [R15].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [R6]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R14]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [R4], namely (i) PACE or BAC and (ii) Passive Authentication with SO.D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this PP the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
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.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [R6] (there "Machine readable travel document").
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [R15] and programmed according to the Logical Data Structure as specified by ICAO, [R6], sec III.
Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.

User data	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [R5] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE . CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [R2]).
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. [R6]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
EAC	Extended Access Control
EF	Elementary File
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
PT	Personalisation Terminal
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SIP *TA*	Standard Inspection Procedure Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)

12 Bibliography

[R1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
[R2]: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
[R3]: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012
[R4]: ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010
[R5]: Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012
[R6]: International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, 2006 (this includes the latest Supplemental for ICAO Doc 9303 which also should be considered)
[R7]: Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 MA-02, Version 1.3.2, December 2012
[R8]: Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009
[R9]: Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007
[R10]: Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[R11]: ISO/IEC 11770-3: Information technology — Security techniques — Key management-- Part 3: Mechanisms using asymmetric techniques, 2008
[R12]: PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993
[R13]: Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009
[R14]: ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008
[R15]: ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[R16]: Common Criteria Protection Profile Machine Readable using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01,Version 1.01, July 2014
[R17]: ISO/IEC 15946-2: Information technology — Security techniques —Cryptographic techniques based on elliptic curves: Part2-Digital signatures
[R18]: PKCS #1: RSA Cryptographic Standard, RSA Laboratories Version 2.1, June 14, 2002
[R19] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Reaffirmed 1999 October 25
[R20] Composite product evaluation for Smart Cards and similar devices September 2007 Version 1.0 Revision 1

Index