OBERTHUR TECHNOLOGIES

ePass v3 TD
Taranis

EAC on SAC passport

Public Security Target

Table of contents

List of tables

List of figures

1 Introduction

1.1 Security Target reference

1.1.1 General identification

Title:	TARANIS Security Target
Reference:	FQR 110 6667
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL5 + ALC_DVS.2 + AVA_VAN.5
PP(s):	BSI-CC-PP-0056-V2-2012 Machine Readable Travel Document with ”ICAO Application”, Extended Access Control with PACEV2 (EAC PP) [R8] BSI-CC-PP-0068-V2-2011 Machine Readable Travel Document using Standard Inspection Procedure with PACEV2 [R7]
ITSEF:	Serma Technologies
Certification Body:	ANSSI
Evaluation scheme:	FR

Table 1: General identification

1.1.2 TOE technical identification

Name:	ID-One ePass V3 TD in EAC on SAC configuration with Active Authentication
SAAAAR Rom code:	079161
SAAAAR Optional code:	079223

Table 2: TOE technical identification

1.1.3 IC identification

IC Reference:	**P5CD081/P5CC081/P5CD041 V1A**
IC EAL:	EAL5 + ALC_DVS.2 + AVA_VAN.5
IC Certificate:	BSI-DSZ-CC-0555-2009
Chip Manufacturer:	NXP Semiconductors

Table 3: IC identification

2 Target Of Evaluation description

2.1 Target Of Evaluation Overview

2.1.1 TOE type

The current document aims at defining the functions and assurance security requirements which apply to the TARANIS project.

TARANIS is a composite product, composed with an Integrated Circuit (IC) and an embedded software providing secure data management following eMRTD specifications (TR 03110 v2.10 [R3] part 1 & TR SAC v1.01 [R2]).

The TOE is a versatile device that can be easily configured in order to operate in different modes including PACEV2, EAC as well as Active Authentication security features. It possesses a dual interface to perform contact and contactless communications.

The Target Of Evaluation addressed in this Security Target is conformant to the Protection Profiles PP 0056v2 [R8] and PP 0068v2 [R7]. As mentioned in those PPs, the BAC is not usable in the TOE.

This device can also be proposed as a ID1 card or an inlay to be integrated in secure document booklet.

2.1.2 Logical scope

The Target of Evaluation (TOE) is a smartcard composed of the following components:

- P5CD081, P5CC081 or P5CD041 NXP chips
- Native “BIOS” allowing efficient access to chip functionalities
- Dedicated highly secure cryptographic library
- Resident application, on top of the BIOS for the personalization
- LDS application providing both the PACEV2 and EAC features on top of the BIOS

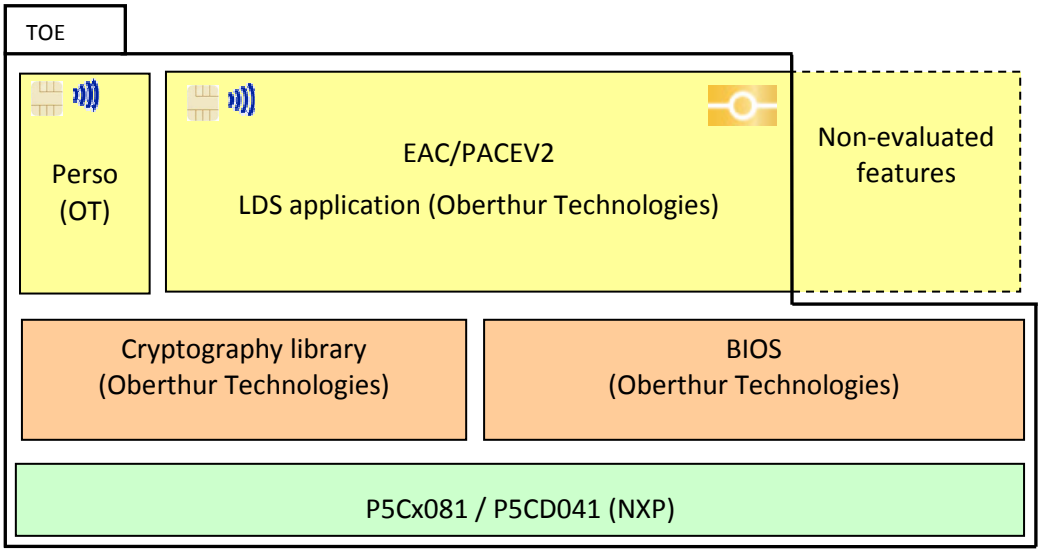

Figure 1: TOE architecture

2.1.2.1 Integrated Circuit (IC)

The TOE relies on the functional and security features of the P5CD081, P5CC081 and P5CD041. This chip is designed to embed the secure code of Oberthur Technologies for the production of smart cards.

This chip provides the following major features:

- Die integrity
- Monitoring of environmental parameters
- Protection mechanisms against faults
- FameXE Enhanced Public key coprocessor especially for RSA and ECC
- 3DES coprocessor
- AES coprocessor
- AIS-31 class P2 compliant Random Number Generator
- CRC calculation block

For more details, see [R12].

2.1.2.2 Basic Input/Output System (BIOS)

The native BIOS provides an efficient and easy way to access chip features from the applications. Indeed, it is based on services organized according to a multi-layer design which allows applications to use a high level interface completely independent of the chip.

The main features of the OS are the following:

- EEPROM management including secure data processing
- Other memories management
- Transaction management
- APDU protocol management
- Low level T=0 ; T=1 and T=CL management
- Error processing
- Advanced securities activation

2.1.2.3 Resident application

This application manages the TOE in pre-personalisation, personalisation and use phase in order to configure the card in the expected way.
It implements and controls access to the following services:

- MSK management
- File management including data reading and writing
- Key generation
- Key injection
- PIN management
- Locks management

The resident application can be addressed:

- In clear mode for secure environment or non-sensitive commands.
- Using a 3DES or AES secure channel otherwise.

2.1.2.4 LDS application

The Logical Data Structure (LDS) application is a generic filesystem that can be configured to match especially ICAO specifications for eMRTDs PACEV2 and EAC.
It also includes commands and protocol management specified in [R13] used to grant access to sensitive data stored in the filesystem.

2.1.2.4.1 Password Authenticated Connection Establishment (PACEV2)

The Password Authenticated Connection Establishment (PACEV2) is a security feature that is supported by the TOE.

The Inspection System:

- Reads the printed data in the MRZ (for eMRTD) or the CAN (the holder may as well enter it itself).
- Authenticates itself as Inspection System by means of keys derived from MRZ or CAN data. After successful 3DES based authentication, the TOE provides read access to data requiring PACEV2 rights by means of a private communication (secure messaging) with the Inspection System.

2.1.2.4.2 Active Authentication (AA)

The Active Authentication of the TOE is an optional feature that may be implemented. It ensures that the TOE has not been "cloned", by means of a challenge-response protocol between the Inspection System and the TOE. For this purpose the chip contains its own Active Authentication RSA or ECC Key pair. A hash representation of Data Group 15 and optionally 14 (DG14/DG15, see 3.1.1) containing the Verification Public Key and attributes (algorithm...) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is stored in the TOE's secure memory.
The TOE supports the loading and generation of the Active Authentication RSA or ECC Key pair.

2.1.2.4.3 Extended Access Control (EAC)

The Extended Access Control (EAC) enhances the later security features and ensures a strong and mutual authentication of the TOE and the Inspection System. This step is required to access biometric data such as fingerprints and iris stored in DG3 and DG4.

The Extended Access Control authentication steps which are implemented by the TOE may be performed either with elliptic curve cryptography, or with DH/RSA cryptography.

2.1.3 Physical scope

The TOE is made of the following part:

- P5CD081, P5CC081 and P5CD041 NXP chips
- Features described in the table below

Feature	Embedded?	TOE scope?	References
BAC***	✔	✘	[R3], [R4]
PACEV2	✔	✔	[R2], [R3], [R4]
EAC	✔	✔	[R2], [R3], [R4]
Active Authentication*	✔	✔	[R2], [R4]
Cryptosystem migration**	✔	✔	[R2], [R3], [R4]
BAP	✔	✘	[R6], [R7], [R8]
EAP	✔	✘	[R6], [R7], [R8]
Patch Mechanism	✔	✔	[R31]

Table 4: Physical scope

* (RSA CRT/SFM and ECC)
** (Algorithm change during certificate verification transaction)
*** The feature BAC is also evaluated, but described in a separate security target.

2.1.3.1 Physical overview

Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.

This device can have different physical configurations, such as ID1 card, or inlay to integrate in secure document booklet.

2.1.4 Non-TOE hardware/software/firmware

Some features of the product are put out of the evaluation scope and are therefore not part of the TOE. Here is the complete list of those functionalities:

- Basic Access Control (required)
- BAP and EAP protocols
- Standard and biometric PIN management (therefore PIN associated commands are out of scope)
- Watermarking feature

2.1.5 Usage and major security features of the TOE

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 security target contains:

- Visual (eye readable) biographical data and portrait of the holder
- Separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
- 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:

- Possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and
- 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 Security Target the travel document is viewed as unit of:

- **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
  - the biographical data on the biographical data page of the travel document surface,
  - the printed data in the Machine Readable Zone (MRZ) and
  - the printed portrait

- **The logical travel document** has data of the travel document holder stored according to the Logical Data Structure as defined in [6] 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:
  - Digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  - Digitized portraits (EF.DG2),
  - Biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
  - Other data according to LDS (EF.DG5 to EF.DG16) and
  - 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) [6].

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 [6], and Password Authenticated Connection Establishment [4].

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 in:

- Integrity by write-only-once access control and by physical means, and
- Confidentiality by the Extended Access Control Mechanism.

The TOE addresses the Chip Authentication Version 1 described in [5] as an alternative to the Active Authentication stated in [6].

BAC is supported by the TOE. This is due to the fact that [8] 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)' [7]. Note that [7] considers high attack potential.

For the PACE protocol according to [4], the following steps shall be performed:

- 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
- The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data
- 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.
- 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) [5], [4].

The Extended Access Control, implemented by the TOE as defined in [5], consists of two parts:

- the Chip Authentication Protocol Version 1 and
- the Terminal Authentication Protocol Version 1 (v.1).

The Chip Authentication Protocol v.1:

- authenticates the travel document's chip to the inspection system and
- 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 Authenticationv.1 has been successfully executed.
The Terminal Authentication Protocolv.1 consists of:

- the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and
- 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.

2.2 Target Of Evaluation Reference

The TOE is identified as follows:

TOE name (Commercial name)	**ePass V3 TD**
Guidance document for preparation	FQR 110 6450 Ed 1 – TARANIS – AGD_PRE
Guidance document for use	FQR 110 6468 Ed 1 – TARANIS – AGD_OPE
TOE identification (Answer to GET DATA DF66)	079161FF030000000000
Internal Identification	P12-023 - ID One ePass EAC v2 on P5CD081
Configuration management (PVCS) label	ePass_V2.2_EACV2_VERSION_12

Table 5: TOE reference

2.3 Life cycle

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to the [9], the TOE life-cycle is additionally subdivided into 7 steps.)

The table below presents the TOE role:

Roles	**Subject**
IC developer	NXP Semiconductors
IC manufacturer	NXP Semiconductors
Software developer	Oberthur Technologies
Travel document manufacturer	Oberthur Technologies or another agent
Prepersonalisation Agent	Oberthur Technologies or another agent
Personalisation Agent	Oberthur Technologies or another agent

Table 6: Roles identification

The table below presents the subjects following TOE life cycle steps, the TOE delivery point and the coverage:

Steps	**Subject**	**Covered by**
Step 1	NXP Semiconductors	IC certification
Step 2	Oberthur Technologies	ALC R&D sites
Step 3	NXP Semiconductors	IC certification
TOE delivery point		
Step 4	Travel Document Manufacturer	AGD_OPE AGD_PRE
Step 5	Travel Document Manufacturer	AGD_OPE AGD_PRE
Step 6	Personalization Agent	AGD_OPE AGD_PRE
Step 7	End user	AGD_OPE AGD_PRE

Table 7: Subjects identification following Life cycle steps

Phase 1 "Development"

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the eMRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the eMRTD application and the guidance documentation is securely delivered to the travel document manufacturer.

Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacture to the travel document manufacturer. If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

TOE delivery point

(Step4) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the card only.

(Step5) The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories if necessary, (ii) creates the eMRTD application, and (iii) equips travel document's chips with pre-personalization Data.

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

Phase 3 "Personalisation of the travel document"

(Step6) The personalisation of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the personalization of the visual readable data onto the physical part of the travel document, (iv) the writing of the TOE User Data and TSF Data into the logical travel document and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object. The signing of the Document security object by the Document signer [6] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

Phase 4 “Operational Use”

(Step7) The TOE is used as a travel document'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 Organisation and can be used according to the security policy of the issuing State but they can never be modified.

Note that the personalisation process and its environment may depend on specific security needs of an issuing State or Organisation. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalisation and the related security objectives into aspects relevant before vs. after TOE delivery. Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

2.4 Conformance claim

This security target claims conformance to the Common Criteria version 3.1, revision 4.
The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict Conformance
Part 2	Conformance to the extended part: - FAU_SAS.1: "Audit storage" - FCS_RND.1: "Quality metric for random numbers" - FMT_LIM.1: "Limited capabilities" - FMT_LIM.2: "Limited availability" - FPT_EMS.1: "TOE emanation" - FIA_API.1: Authentication Proof of Identity"
Part 3	Conformance to EAL5, augmented with: - AVA_VAN.5: “Advanced methodical vulnerability analysis” - ALC_DVS.2: “Sufficiency of security measures”

Table 8: TOE conformance claim

Nota bene:
SAR additions have been chosen, following the Protection Profile requirements, more information are available in § 2.6.4.2.

2.5 Protection Profile Reference

This security target claims a strict conformance to the following protection profiles:

- BSI-CC-PP-0056-V2-2012: “Machine Readable Travel Document with ”ICAO Application”, Extended Access Control with PACEV2 (EAC PP)”
- BSI-CC-PP-0068-V2-2011:”Machine Readable Travel Document using Standard Inspection Procedure with PACEV2”

2.6 Conformance claim rationale

The TOE described in this Security Target is in conformance with the TOE type described in the two protection profiles.

The security problem definition of this Security Target is consistent with the one in the two PP, as it was extracted from it. No organisational security policies or assumption have been added. One threat regarding the patch loading has been added to the security target, and one objective has been added for covering this threat.

The ALC scope of evaluation encompasses phase 1 and phase 2 of the PP life cycle. Part of phase 2 and phases 3 and 4 are covered by AGD, as described in the previous chapter.

As required in PP0056 v2, the TOE claims a strict conformance to PP0056 v2.
As required in PP0068 v2, the TOE claims a strict conformance to PP0068 v2.

The TOE evaluation level assurance is conformant to the ones claimed in the two Protection Profiles.

Classes	**Familly**	**PP**	**TOE**
Development	ADV_ARC	1	1
	ADV_FSP	4	5
	ADV_IMP	1	1
	ADV_INT	-	2
	ADV_SPM	-	-
	ADV_TDS	3	4
Guidance documents	AGD_OPE	1	1
	AGD_PRE	1	1
Life-cycle support	ALC_CMC	4	4
	ALC_CMS	4	5
	ALC_DEL	1	1
	ALC_DVS	2	2
	ALC_FLR	-	-
	ALC_LCD	1	1
	ALC_TAT	1	2
Security Target	ASE_CCL	1	1
	ASE_ECD	1	1
	ASE_INT	1	1
	ASE_OBJ	2	2
	ASE_REQ	2	2
	ASE_SPD	1	1
	ASE_TSS	1	1
Tests	ATE_COV	2	2
	ATE_DPT	2	3
	ATE_FUN	1	1
	ATE_IND	2	2
Vulnerability assessment	AVA_VAN	5	5

Table 9: SAR consistency

3 Security problem definition

3.1 Assets

3.1.1 User data

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 PACEV2 PP [R7], chap 3.1.

Logical travel document sensitive User Data

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

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.

Due to strict conformance to PACEV2 PP, this ST also includes all assets listed in [R7], chap 3.1, 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).

They are refined here below for the present TOE.

User data stored on the TOE

All data (being not authentication data) stored in the context of the eMRTD application of the travel document as defined in [R2] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACEV2 (in the sense of [R2]), i.e. for the current TOE:

CPLC Data	Data uniquely identifying the chip. They are considered as user data as they enable to track the holder
Sensitive biometric reference data (EF.DG3, EF.DG4)	Contain the fingerprint and the iris picture
Chip Authentication Public Key and attributes in EF.DG14	Contain public data enabling to authenticate the chip thanks to a chip authentication
Active Authentication Public Key and attributes in EF.DG15	Contain public data enabling to authenticate the chip thanks to an active authentication

Table 10: User data stored on the TOE

Property to be maintained by the current security policy: Confidentiality, Integrity and Authenticity.

Though not each data element stored on the TOE represents a secret, the specification [4] anyway requires securing their confidentiality: only terminals authenticated according to [4] can get access to the user data stored. They have to be operated according to P.Terminal.

User data transferred between the TOE and the terminal connected

All data (being not authentication data) being transferred in the context of the eMRTD application of the travel document as defined in [R2] between the TOE and an authenticated terminal acting as Basic Inspection System with PACEV2 (in the sense of [R2]).

User data can be received and sent (exchange <--> [receive, send]).

Property to be maintained by the current security policy: Confidentiality, Integrity and Authenticity.

Though not each data element being transferred represents a secret, the specification [4] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [4].

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 PACEV2 password. TOE tracing data can be provided / gathered.

Property to be maintained by the current security policy: Unavailability

Unavailability represents a prerequisite for anonymity of the travel document holder

3.1.2 TSF data

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.

Personalisation Agent reference authentication Data	Private key enabling to authenticate the Personalisation agent (same as PACEV2 ST)
Password Authenticated Connection Establishment (PACEV2) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document (same as PACEV2 ST)
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity

Table 11: Accessibility to the TOE functions and data only for authorised subjects

Property to be maintained by the current security policy: Availability.

Genuineness of the TOE

Property of the TOE is to be authentic in order to provide claimed security functionality in a proper way. The authenticity of the MRTD's chip personalised by the issuing State or Organization for the

MRTD holder is used by the traveller to prove his possession of a genuine MRTD. This asset also covers "Authenticity of the MRTD's chip" in [R9].

TOE_ID	Data enabling to identify the TOE
Chip Authentication private Key	Private key the chip uses to perform a chip authentication
Active Authentication private key	Private key the chip uses to perform an active authentication
Current Date	Current date of the travel document

Table 12: Genuineness of the TOE

Property to be maintained by the current security policy: Availability.

TOE internal secret cryptographic keys

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

Personalisation Agent reference authentication Data	Private key enabling to authenticate the Personalisation agent
Password Authenticated Connection Establishment (PACEV2) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Chip Authentication private Key	Private key the chip uses to perform a chip authentication
Active Authentication private key	Private key the chip uses to perform an active authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity
MSK	Manufacturer Secret Key used to perform the authentication of the personal agent in pre-personalisation phase
LSK	Loading Secure Key used to load Optional Code in pre-personalisation phase

Table 13: TOE internal secret cryptographic keys

Property to be maintained by the current security policy: 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.

TOE_ID	Data enabling to identify the TOE and the TOE Configuration
Life Cycle State	Life Cycle state of the TOE
Public Key CVCA	Trust point of the travel document stored in persistent memory
CVCA Certificate	All the data related to the CVCA key (expiration date, name,..) stored in persistent memory
Current Date	Current date of the travel document

Table 14: TOE internal non-secret cryptographic material

Property to be maintained by the current security policy: Integrity, Authenticity.

Travel Document communication establishment authorisation data

Restricted-revealable authorization information for a human user being used for verification of the authorisation attempts as authorised user (PACEV2 password). These data are stored in the TOE and are not to be send to it.

PACEV2 password (MRZ or CAN)	Reference information being persistently stored in the TOE and allowing PACEV2 authentication

Table 15: Travel Document communication establishment authorisation data

Property to be maintained by the current security policy: Confidentiality, Integrity.

3.2 Users / Subjects

This ST encompasses the subjects from PP0056 v2 and PP0068 v2.

Role	Definition
Attacker	Additionally to the definition from PACEV2 PP [R7], 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

Role	Definition
Basic Inspection System with PACE(BIS-PACE)	A technical system being used by an inspecting authority 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.
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 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. [6], 5.5.1
Country Verifying Certification Authority (CVCA)	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 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 (CDS). This role is usually delegated to a Personalisation Agent
Document Verifier	The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in form of the Document Verifier Certificates

Role	Definition
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining a 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 PACEV2 and/or BAC; (iii) gets the authorization to read the logical travel document either under PACEV2 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 [R3] 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 PACEV2 and BAC are supported by the TOE and the BIS, PACEV2 must be used
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
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 [6], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [6](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.
Terminal	A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [9]

Role	Definition
Travel document holder	A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [9].Please note that a travel document holder can also be an attacker
Travel document presenter	A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [9].Please note that a travel document presenter can also be an attacker

Table 16: Users / Subjects

3.3 Threats

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

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

T.Read_Sensitive_Data

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. [R10]) 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 PACEV2 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 Travel Document as well.

Threat agent: having high attack potential, knowing the PACEV2 Password, being in possession of a legitimate Travel Document.

Asset: confidentiality of logical Travel Document sensitive user data (i.e. biometric reference).

T.Counterfeit

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 on 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.

T.Skimming

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 (PACEV2 password) in advance.

Asset: confidentiality of logical travel document data

T.Eavesdropping

Adverse action: An attacker is listening to the communication between the travel document and the PACEV2 authenticated BIS-PACEV2 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 (PACEV2 password) in advance.

Asset: confidentiality of logical travel document data

T.Tracing

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 (PACEV2 password) in advance.

Asset: privacy of the travel document holder

T.Forgery

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 PACEV2 authenticated BIS-PACEV2 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

T.Abuse-Func

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

T.Information_Leakage

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

T.Phys-Tamper

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

T.Malfunction

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

3.3.1 Additional threat

T.PATCH_LOADING

The attacker tries to avoid the loading of a genuine patch, alter a patch (during loading or once loaded), or to exploit the patch loading mechanism to load unauthenticated code on the TOE, in order to get access to the assets, the TSF data or the TOE user data, or to modify the TSF.

3.4 Organisational Security Policies

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).

P.Sensitive_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

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical 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 Organization only.

P.Manufact

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

1) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
2) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE27.

3) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 above.
4) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

P.Card_PKI

1) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA);
2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [R2], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [R2], 5.5.1.
3) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworthy_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

The Basic Inspection Systems with PACEV2 (BIS-PACEV2) shall operate their terminals as follows:

1) The related terminals shall be used by terminal operators and by travel document holders.
2) They shall implement the terminal parts of the PACEV2 protocol [R2], of the Passive Authentication [R4] and use them in this order. The PACEV2 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, [R4]).
5) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACEV2 passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

3.5 Assumptions

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

A.Insp_Sys

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACEV2 [R2] and/or BAC [R9]. BAC may only be used if supported by the TOE. If both PACEV2 and BAC are supported by the TOE and the IS, PACEV2 must be used. The EIS reads the logical travel document under PACEV2 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 PP PACEV2 [R7] 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

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their 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 PACEV2 part of the TOE nor will the security objectives of the [R7] 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.

A.Passive_Auth

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical Travel Document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the Travel Documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [R2].

4 Security Objectives

4.1 Security Objectives for the TOE

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

OT.Sens_Data_Conf

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

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 Organization by means of the Chip Authentication Version 1 as defined in [R10]. The authenticity proof provided by Travel Document's chip shall be protected against attacks with high attack potential.

OT.Data_Integrity

The TOE must ensure integrity of the User Data and the TSF-data 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 PACEV2 authenticated BIS-PACEV2) after the PACEV2 Authentication.

OT.Data_Authenticity

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side.

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 PACEV2 authenticated BIS-PACEV2) after the PACEV2 Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACEV2 authenticated BIS-PACEV2 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 PACEV2 authenticated BIS-PACEV2) after the PACEV2 Authentication.

OT.Tracing

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 (PACEV2 passwords) in advance.

OT.Prot_Abuse-Func

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

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.

OT.Prot_Phys-Tamper

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the Travel Document's Embedded Software by means of measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis) manipulation of the hardware and its security features, as well as controlled manipulation of memory contents (User Data, TSF Data) with a prior reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction

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

The TOE must provide means to store Identification (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 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.AC_Pers

The TOE must ensure that the logical Travel Document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [R4] 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 its personalisation.

4.1.1 Additional objective

OT.Patch_Loading

The TOE shall provide a secure patch code loading mechanism

OT.Chip_Authenticity

The TOE must support the Inspection Systems to verify the authenticity of the Travel Document's chip. The TOE stores a RSA or ECC private key to prove its identity, and that is used in chip authentication. This mechanism is described as "Active Authentication".

4.2 Security objectives for the Operational Environment

4.2.1.1 Issuing State or Organization

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

OE.Auth_Key_Travel Document

The issuing State or Organization 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 organizations to verify the authenticity of the Travel Document's chip used for genuine Travel Document by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE. Authoriz_Sens_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.

4.2.2 Receiving State or Organization

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

OE.Exam_Travel Document

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveler 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 PACEV2 [R2] and/or the Basic Access Control [R4]. Extended Inspection Systems perform

additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

OE.Prot_Logical_Travel_Document

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

OE.Ext_Insp_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.

4.2.2.1 Travel document Issuer as the general responsible

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

OE.Legislative_Compliance

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

4.2.2.2 Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment:

OE.Passive_Auth_Sign

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. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data. 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

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) enroll the biometric reference data of the travel document holder, (iii)

write a subset of these data on the physical MRTD (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [2], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [2](in the role of a DS).

4.2.2.3 Terminal operator: Terminal's receiving branch

OE.Terminal

The terminal operators must operate their terminals as follows:

- The related terminals are used by terminal operators and by travel document holders.
- The related terminals implement the terminal parts of the PACEV2 protocol, of the Passive Authentication (by verification of the signature of the Document Security Object) and use them in this order. The PACEV2 terminal uses randomly and (almost)for Diffie-Hellmann).
- The related terminals need not to use any own credentials.
- The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document).
- The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACEV2 passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

4.2.2.4 Travel document holder Obligations

OE.Travel_Document_Holder

The travel document holder may reveal, if necessary, his or her verification values of the PACEV2 password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

5 Extended requirements

5.1 Extended families

5.1.1 Extended family FAU_SAS - Audit data storage

5.1.1.1 Description

see [R7], §5.1 for more details.

5.1.1.2 Extended components

5.1.1.2.1 Extended component FAU_SAS.1

Description

see [R7], §5.1 for more details.

Definition

FAU_SAS.1 Audit storage

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.

Dependencies: No dependencies.

Rationale

see [R7], §5.1 for more details.

5.1.1.3 Rationale

see [R7], §5.1 for more details.

5.1.2 Extended family FCS_RND - Generation of random numbers

5.1.2.1 Description

see [R7], §5.2 for more details.

5.1.2.2 Extended components

5.1.2.2.1 Extended component FCS_RND.1

Description

See [R7], §5.2 for more details.

Definition

FCS_RND.1 Quality metric for random numbers

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

Dependencies: No dependencies.

Rationale

See [R7], §5.2 for more details.

5.1.2.3 Rationale

see [R7].

5.1.3 Extended family FMT_LIM - Limited capabilities and availability

5.1.3.1 Description

See [R7], §5.3 for more details.

5.1.3.2 Extended components

5.1.3.2.1 Extended component FMT_LIM.1

Description

See [R7], §5.3 for more details.

Definition

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 [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.2)

Rationale

See [R7], §5.3 for more details.

5.1.3.2.2 Extended component FMT_LIM.2

Description

See [R7], §5.3 for more details.

Definition

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 [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.1)

Rationale

See [R7], §5.3 for more details.

5.1.3.3 Rationale

See [R7], §5.3 for more details.

5.1.4 Extended family FPT_EMS - TOE Emanation

5.1.4.1 Description

See [R7], §5.4 for more details.

5.1.4.2 Extended components

5.1.4.2.1 Extended component FPT_EMS.1

Description

See [R7], §5.4 for more details.

Definition

FPT_EMS.1 TOE Emanation

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].

Dependencies: No dependencies.

Rationale

See [R7], §5.4 for more details.

5.1.4.3 Rationale

See [R7], §5.4 for more details.

5.1.5 Extended family FIA_API - Authentication Proof of Identity

5.1.5.1 Description

See [R8], §5.1 for more details.

5.1.5.2 Extended components

5.1.5.2.1 Extended component FIA_API.1

Description

See [R8], §5.1 for more details.

Definition

FIA_API.1 Authentication Proof of Identity

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

Dependencies: No dependencies.

Rationale

See [R8], §5.1 for more details.

5.1.5.3 Rationale

See [R8], §5.1 for more details.

6 Security Functional Requirements

6.1 Security Functional Requirements

Definitions of security attributes, keys and certificated referred in this section can be found in [R8], §6.

6.1.1 SFR from PP0056v2 and PP0068v2

6.1.1.1 Class FAU Security Audit

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **the IC the Initialisation and Pre-Personalisation Data** in the audit records.

6.1.1.2 Class FCS Cryptographic Support

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following:

Iteration	Algorithm	Standard	Key size
DH_PACE	ECDH protocol	[R14]	128, 192, 256 bits
CA	Diffie-Hellman key derivation protocol	[R19] and [R3]	128, 192, 256 bits
	ECDH protocol	[R14]	128, 192, 256 bits

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 **zeroisation** that meets the following: **none**.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignement: list of standards]**

Iteration	Operation	Algorithm	Key Size	Standard
PACEV2_ENC	SM, encryption, decryption	AES CBC with dynamic ICV	128, 192 or 256 bits	ISO 10116
		3DES CBC	112 bits	FIPS 46-3,FIPS 197
CA_ENC	SM, encryption, decryption	AES CBC with dynamic ICV	128, 192 or 256 bits	ISO 10116
		3DES CBC	112 bits	FIPS 46-3,FIPS 197

Iteration	Operation	Algorithm	Key Size	Standard
PACEV2_MAC	SM, MAC	Retail MAC with 3DES	112 bits	ISO 9797 (MAC Algorithm 3 block cipher DES, Sequence Message Counter, padding mode 2)
		C-MAC AES	128, 192 and 256 bits	NIST-838B
CA_MAC	SM, MAC	Retail MAC with 3DES	112 bits	ISO 9797 (MAC Algorithm 3 block cipher DES, Sequence Message Counter, padding mode 2)
		C-MAC AES	128 bits, 192 bits 256 bits	NIST-838B
SIG_VER_RSA	digital signature verification	RSA with SHA1, SHA-256 or SHA-512	1024 to 2048 bits	PKCS#1 v1.5 PKCS#1 v2.1 (PSS)
SIG_VER_ECC	digital signature verification	ECDSA with SHA1, SHA-224, SHA-256, SHA-384 or SHA-512	192 to 521 bits over characteristic p curves for ECC	[R14]
AA	digital signature creation for Active Authentication	RSA CRT or RSA SFM with SHA1, SHA-224, SHA-256, SHA-384 or SHA-512	1024 to 2048 bits (by steps of 256bits)	scheme 1 of [R18]
		ECDSA with SHA1, SHA-224, SHA-256, SHA-384 or SHA-512	192, 256, 384 and 521 bits	[R15], [R16], [R17]

.

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **the requirement provided in RGS_B1, using chip AIS31 class P2 [R35]**

Application note: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACEV2) as required by FIA_UAU.4/PACEV2

6.1.1.3 Class FIA Identification and Authentication

The table below provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Authentication Mechanism for Personalisation Agents	FIA_UAU.1/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

FIA_AFL.1/PACEV2 Authentication failure handling

FIA_AFL.1.1/PACEV2 The TSF shall detect when **an administrator configurable positive integer within 1 to 255 consecutive** unsuccessful authentication attempts occur related to **PACEV2 authentication protocol**.

FIA_AFL.1.2/PACEV2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **wait for an increasing time between receiving of the terminal challenge and sending of the TOE response during the PACEV2 authentication attempts**.

FIA_UID.1/PACEV2 Timing of identification

FIA_UID.1.1/PACEV2 The TSF shall allow

- **1. to establish a communication channel**
- **2. carrying out the PACEV2 Protocol according to [R2]**
- **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 [R3]**
- **5. to carry out the Terminal Authentication Protocol v.1 according to [R3]**

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

FIA_UID.1.2/PACEV2 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/PACEV2 in the current ST covers the definition in PACEV2 PP [R7] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACEV2 PP.

Application note: User identified after a successfully performed PACEV2 protocol is a PACEV2 authenticated BIS-PACEV2. Please note that neither CAN nor MRZ effectively represent secrets (but other PACEV2 passwords may do so), but are restricted-revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACEV2).

FIA_UAU.1/PACEV2 Timing of authentication

FIA_UAU.1.1/PACEV2 The TSF shall allow

- **1. to establish a communication channel**
- **2. carrying out the PACEV2 Protocol according to [R2]**
- **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 v.1 according to [R3]**
- **6. to carry out the Terminal Authentication Protocol v.1 according to [R3]**

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

FIA_UAU.1.2/PACEV2 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/PACEV2. in the current ST covers the definition in PACEV2 PP [R7] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACEV2 PP.

Application note: The user authenticated after a successfully performed PACEV2 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-PACEV2). If PACEV2 was successfully performed, secure messaging is started using the derived session keys (PACEV2-K_{MAC}, PACEV2-KEnc), cf. FTP_ITC.1/PACEV2.

FIA_UAU.4/PACEV2 Single-use authentication mechanisms

FIA_UAU.4.1/PACEV2 The TSF shall prevent reuse of authentication data related to

- **1. PACEV2 Protocol according to [R2]**
- **2. Authentication Mechanisms based on Triple-DES and AES**
- **3. Terminal Authentication Protocol v.1 according to [R3]**

Application note: The SFR FIA_UAU.4.1 in the current ST covers the definition in PACEV2 PP [R7] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACEV2 PP. The generation of random numbers (random nonce) used for the authentication protocol (PACEV2) and Terminal Authentication as required by FIA_UAU.4/PACEV2 is required by FCS_RND.1 stated in this ST.

FIA_UAU.5/PACEV2 Multiple authentication mechanisms

FIA_UAU.5.1/PACEV2 The TSF shall provide

- **1. PACEV2 Protocol according to [R2]**

- **2. Passive Authentication according to [R4]**
- **3. Secure messaging in MAC-ENC mode according to [R2]**
- **4. Symmetric Authentication Mechanism based on Triple-DES and AES**
- **5. Terminal Authentication Protocol v.1 according to [R3]**

to support user authentication.

FIA_UAU.5.2/PACEV2 The TSF shall authenticate any user's claimed identity according to the

- **1. Having successfully run the PACEV2 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 PACEV2 protocol**
- **2. The TOE accepts the authentication attempt as Personalisation Agent by**
  - **the Symmetric Authentication Mechanism with Personalisation Agent Key**
- **3. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1,**
- **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.**

Application note: The SFR FIA_UAU.5.1/PACEV2 in the current ST covers the definition in PACEV2 PP [R7] and extends it by EAC aspects 4) and 5). The SFR FIA_UAU.5.2/PACEV2 in the current ST covers the definition in PACEV2 PP [R7] and extends it by EAC aspects 3) and 4). These extensions do not conflict with the strict conformance to PACEV2 PP.

Application note: Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of eMRTDeMRTD application.

FIA_UAU.6/PACEV2 Re-authenticating

FIA_UAU.6.1/PACEV2 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the PACEV2 protocol shall be verified as being sent by the PACEV2 terminal**.

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.**

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **Chip Authentication Protocol Version 1 according to [R3]** to prove the identity of the **TOE**.

6.1.1.4 Class FDP User Data Protection

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 31: The SFR FIA_ACC.1.1 in the current ST covers the definition in PACEV2 PP [R7] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACEV2 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:**
  - **a. Terminal**
  - **b. BIS-PACEV2**
  - **c. Extended Inspection System**
- **2. Objects:**
  - **a. data EF.DG1, EF.DG2, EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical Travel Document,**
  - **b. data in EF.DG3 of the logical Travel Document**
  - **c. data in EF.DG4 of the logical Travel Document**
  - **d. all TOE intrinsic secret cryptographic keys stored in the travel document[1],**
- **3. Security attributes:**
  - **a. PACEV2 authentication**
  - **b. Terminal Authentication Version 1**
  - **c. Authorization of the Terminal**

[1] E.g. Chip Authentication Version 1 and ephemeral keys or Active Authentication public key

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-PACEV2 is allowed to read data objects from FDP_ACF.1.1/TRM according to [R2] after a successful PACEV2 authentication as required by FIA_UAU.1/PACEV2.**

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 PACEV2 authenticated BIS-PACEV2 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**

7. Terminals authenticated are able to establish a SM for dealing with DG.3 & DG.4, regarding to the SM level defined in personalisation, by the personalisation agent

Application note: The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACEV2 PP [R7] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACEV2 PP [R7]. The SFR FDP_ACF.1.4/TRM in the current PP covers the definition in PACEV2 PP [R7] and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACEV2 PP.

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:

- **Session Keys (immediately after closing related communication session)**
- **the ephemeral private key ephem-SK_{PICC}-PACEV2 (by having generated a DH shared secret K)**.

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.

6.1.1.5 Class FMT Security Management

FMT_SMF.1 Specification of Management Functions

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

- **1. Initialization (phase 4)**
- **2. Pre-personalisation (phase 5)**
- **3. Personalisation (phase 6)**
- **4. Configuration (phase 6)**

FMT_SMR.1/PACEV2 Security roles

FMT_SMR.1.1/PACEV2 The TSF shall maintain the roles

- **1. Manufacturer, Initialization**
- **2. Personalisation Agent, Pre-personalisation, personalisation and configuration**
- **3. Terminal, use phase**
- **4. PACEV2 authenticated BIS-PACEV2, use phase**
- **3. Country Verifying Certification Authority, use phase**
- **4. Document Verifier, use phase**
- **5. Domestic Extended Inspection System, use phase**
- **6. Foreign Extended Inspection System, use phase**

FMT_SMR.1.2/PACEV2 The TSF shall be able to associate users with roles.

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**

FMT_MTD.1/INI_ENA Management of TSF data

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

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 **Initialization Data and Pre-personalisation Data** to **the Personalisation Agent**.

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**

to **the Personalisation Agent**.

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**

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**

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 **the Personalisation Agent**.

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 (SOD)** to **the Personalisation Agent**.

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. PACEV2 passwords**
- **2. Chip Authentication Private key**
- **3. Personalisation Agent Keys**
- **4. Active Authentication private key**

to **none**.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for **TSF data of the Terminal Authentication Protocol 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 Document Verifier Certificate is not before the Current Date of the TOE,
- (3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

6.1.1.6 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **Power consumption and any kind of side channels during command execution** in excess of **levels that could be analysed in the current state of the art** enabling access to

- **1. Chip Authentication Session Keys**
- **2. PACEV2 session Keys (PACEV2-K_{MAC}, PACEV2-K_{Enc})**
- **3. Ephemeral private key ephem SK_{PICC}-PACEV2**
- **4. Active Authentication private key**
- **5. Personalisation Agent Key(s)**
- **6. Chip Authentication Private Key**

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. PACEV2 session Keys (PACEV2-K_{MAC}, PACEV2-K_{Enc})**

- **3. Ephemeral private key ephem SK_{PICC}-PACEV2**
- **4. Active Authentication private key**
- **5. Personalisation Agent Key(s)**
- **6. Chip Authentication Private Key**

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**

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions**

- **At reset**
- **Before the first execution of the optional code,**
- **After the Active Authentication is computed,**
- **Before any cryptographic operation,**
- **When accessing a DG or any EF,**
- **Prior to any use of TSF data,**
- **Before execution of any command,**
- **When performing a PACEV2 authentication,**
- **When using the CVCA Root key,**
- **When verifying a certificate with an extracted public key µ,**
- **When performing the Chip Authentication,**
- **When performing a Terminal authentication**

to demonstrate the correct operation of **the TSF**.

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

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

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.

6.1.1.7 Class FTP Trusted Path/Channels

FTP_ITC.1/PACEV2 Inter-TSF trusted channel

FTP_ITC.1.1/PACEV2 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/PACEV2 The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/PACEV2 The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for **any data exchange between the TOE and the Terminal**.

Application Note:

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

The trusted channel is established after successful performing the PACEV2 protocol (FIA_UAU.1/LDS). If the PACEV2 was successfully performed, secure messaging is immediately started using the derived session keys (PACEV2-K_{MAC}, PACEV2-KEnc): 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/LDS. The establishing phase of the PACEV2 trusted channel does not enable tracing due to the requirements FIA_AFL.1/LDS.

6.1.2 Additional SFRs for patch loading

The SFR described in this chapter are relative to patch loading. The Patch Loading is only accessible in step 5 of the life cycle, prepersonalisation phase.

FDP_ACC.2/PP Complete access control

FDP_ACC.2.1/PP The TSF shall enforce the **Patch Loading Access Control** on **all subjects and all objects** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/PP The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/PP Security attribute based access control

FDP_ACF.1.1/PP The TSF shall enforce the **Patch Loading Access Control** to objects based on the following **Card Manufacturer Authentication (AS_AUTH_MSK_STATUS)**.

FDP_ACF.1.2/PP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **AS_AUTH_MSK_STATUS=TRUE, via EXTERNAL AUTHENTICATE**.

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

FDP_ACF.1.4/PP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

FIA_UAU.1/PP Timing of authentication

FIA_UAU.1.1/PP The TSF shall allow **INITIALIZE AUTHENTICATION, GET DATA, SELECT FILE** on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1/PP Timing of identification

FIA_UID.1.1/PP The TSF shall allow **INITIALIZE AUTHENTICATION, GET DATA, SELECT FILE** on behalf of the user to be performed before the user is identified.

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

FCS_COP.1/PP Cryptographic operation

FCS_COP.1.1/PP The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following:

Cryptographic operation	Algo	Key length	Standard
Decryption (MSK) and signature verification	DES	112 bits	FIPS-PUB 46-3 (ANSI X3.92), FIPS PUB 81 or ISO/IEC 9797, Data integrity mechanism
Card Manufacturer authentication (MSK)	DES	112 bits	FIPS-PUB 46-3 (ANSI X3.92), FIPS PUB 81 or ISO/IEC 9797, Data integrity mechanism

Cryptographic operation	Algo	Key length	Standard
Card Manufacturer authentication (MSK)	AES	128, 192 and 256 bits	FIPS PUB 197, 26 November 2001
Decryption (of patch ciphered with LSK) and signature verification	AES	128 bits	FIPS PUB 197, 26 November 2001

FTP_ITC.1/PP Inter-TSF trusted channel

FTP_ITC.1.1/PP 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/PP [Editorially Refined] The TSF shall permit **the TOE Developer and Card Manufacturer** to initiate communication via the trusted channel.

FTP_ITC.1.3/PP The TSF shall initiate communication via the trusted channel for **loading the patch code on the card**.

FDP_UIT.1/PP Data exchange integrity

FDP_UIT.1.1/PP The TSF shall enforce the **Patch loading access control SFP** to **receive** user data in a manner protected from **modification** errors.

FDP_UIT.1.2/PP [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification of some of the pieces of the application sent by the TOE developer and Card Manufacturer** has occurred.

Application Note:
Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the patch to be installed on the card to be different from the one sent by the TOE Developer. The Patch loading is performed by the TOE Developer via the command LOAD SECURE, its integrity is ensured by a MAC, described in FCS_COP.1/PP.

FDP_ITC.1/PP Import of user data without security attributes

FDP_ITC.1.1/PP The TSF shall enforce the **Patch loading access control** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/PP The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/PP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FCS_CKM.1/PP Cryptographic key generation

FCS_CKM.1.1/PP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

Cryptographic key generation algorithm	**Cryptographic key size**	**List of standards**
TOE's MSK derived from the MSK loaded in phase 1, using SHA-256	16, 24 and 32 bytes	None

Application Note:
Key derivation algorithm is detailed in AGD_PRE, § Diversified MSK Computation, refer to FQR 110 6468.

FDP_UCT.1/PP Basic data exchange confidentiality

FDP_UCT.1.1/PP The TSF shall enforce the **Patch loading access control** to **receive** user data in a manner protected from unauthorised disclosure.

Application note:
For the Patch loading access control, the LSK is used to cipher the data transmitted.

FMT_MOF.1/PP Management of security functions behaviour

FMT_MOF.1.1/PP The TSF shall restrict the ability to **disable** the functions **LOAD SECURE** to the **Card Manufacturer.**

Application note:
The first operation ensures the irreversible locking of the patch loading feature after pre personalisation state. After this phase, this APDU can not be used.
The last operation permits the loading of patch during phase 5.

FCS_CKM.4/PP Cryptographic key destruction

FCS_CKM.4.1/PP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Key is set to NULL** that meets the following: **none**.

Application Note:
In phase 5, this SFR ensures the secure erasing of the LSK and MSK keys.
In phases 3-4, MSK is diversified during the first command, and then replaced by the new value generated by FCS_CKM.1/PP.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to **prevent** unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that **Patch code identification** stored audit records will be maintained when the following conditions occur: **failure and attack**.

Application Note:
Patch code is loaded with its information and its CRC.
Information on the Patch code is directly retrieved from itself (identification and static signature) and is provided by GET DATA command. This information is protected from modification because the APDU that enable its modification are deactivated after pre personalisation state.

FIA_AFL.1/PP Authentication failure handling

FIA_AFL.1.1/PP The TSF shall detect when **3** unsuccessful authentication attempts occur related to **Card Manufacturer authentication**.

FIA_AFL.1.2/PP When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **always return an error**.

6.1.3 Additional SFRs for SM level configuration

This chapter states the additional security functional requirements that were not already present in the current ST for the need of SM level configuration in use phase for accessing DG.3 and DG.4.

FMT_MSA.1/SM Management of security attributes

FMT_MSA.1.1/SM The TSF shall enforce the **Access Control SFP** to restrict the ability to **modify** the security attributes **Terminal Authentication version 1** to **Personalisation Agent**.

FMT_MSA.3/SM Static attribute initialisation

FMT_MSA.3.1/SM The TSF shall enforce the **Access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SM The TSF shall allow the **Personalisation Agent** to specify alternative initial values to override the default values when an object or information is created.

6.1.4 Additional SFRs for Active Authentication (AA)

This chapter states the additional security functional requirements that were not already present in the current ST for the need of Active Authentication Protocol supported by the TOE.

FDP_DAU.1/AA Basic Data Authentication

FDP_DAU.1.1/AA The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE itself**.

FDP_DAU.1.2/AA The TSF shall provide **any users** with the ability to verify evidence of the validity of the indicated information.

Refinement:

Evidence generation and ability of verfying it, constitute the Active Authentication protocol.

FDP_ITC.1/AA Import of user data without security attributes

FDP_ITC.1.1/AA The TSF shall enforce the **Basic Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/AA The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/AA The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

FMT_MOF.1/AA Management of security functions behaviour

FMT_MOF.1.1/AA The TSF shall restrict the ability to **disable and enable** the functions **TSF Active Authentication** to **Personalisation Agent**.

6.2 Security Assurance Requirements

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

7 TOE Summary Specification

7.1 TOE Summary Specification

SF.ACC_READ Access Control in reading

This function controls access to read functions (in EEPROM) and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state.

It ensures that at any time, the keys are never readable:

- PACEV2 keys,
- Chip authentication keys,
- CVCA public keys,
- Active Authentication private key,
- Personalisation agent keys.

It controls access to the CPLC data as well:

- It ensures the CPLC data can be read during the personalisation phase,
- It ensures it can not be readable in free mode at the end of the personalisation step.

Regarding the file structure:

In the operational use:

- The terminal can read user data (except DG3 & 4), the Document Security Object, the EF.CVCA, EF.COM only after PACEV2 authentication and through a valid secure channel,
- When the EAC was successfully performed, the terminal can only read the DG3 & 4 provided the access rights are sufficient through a valid secure channel.

In the personalisation phase:

- The personalisation agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys).
- The TOE is uniquely identified by a random number, generated at each reset. This unique identifier is called (UID)

It ensures as well that no other part of the EEPROM can be accessed at anytime.

SF.ACC_WRITE Access Control in writing

This function controls access to write functions (in EEPROM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

This security functionality ensures the application locks can only be written once in personalisation phase to be set to "1".

It ensures as well the CPLC data can not be written anymore once the TOE is personalised and that it is not possible to load an optional code or change the personalisation agent authentication keys in personalisation phase.

Regarding the file structure:

- In the operational use:

- It is not possible to create any files (system or data files). Furthermore, it is not possible to update any system files. However the application data is still accessed internally by the application for its own needs, the Root CVCA key files and temporary key files are updated internally by the application according to the authentication mechanism described in [R4].

- In the personalisation phase:
  - The personalisation agent can create and write through a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys).

SF.EAC EAC mechanism

This security functionality ensures the EAC is correctly performed. In particular:

- it handles the certificate verification,
- the management of access rights to DG3 & DG4,
- the management of the current date (update and control towards the expiration date of the incoming certificate),
- the signature verification (in the certificate or in the challenge/response mechanism).

It can only be performed once the TOE is personalised with the chip authentication keys & Root CVCA key(s) the Personalisation Agent loaded during the personalisation phase. Furthermore, this security functionality ensures the authentication is performed as described in [R4].

This security functionality ensures the session keys for secure messaging are destroyed at each successful Chip Authentication step.

The TOE handles an error counter; after several failures in attempting to strongly authenticate the GIS (the error limit is reached). The TOE also implements countermeasures to protect the TOE; it takes more and more time for the TOE to reply to subsequent wrong GIS authentication attempts.

SF.SM Secure Messaging

This security functionality ensures the confidentiality and integrity of the channel between the TOE and the IFD are using to communicate.

After a successful PACEV2 authentication and successful Chip authentication, a secure channel is (re)established based on Triple DES and AES algorithms.

This security functionality ensures:

- No commands were inserted nor deleted within the data flow,
- No commands were modified,
- The data exchanged remain confidential,
- The issuer of the incoming commands and the destinatory of the outgoing data is the one that was authenticated (through PACEV2 or EAC).

If an error occurs in the secure messaging layer, the session keys are destroyed.

SF.AUTH_PERSO Personalisation Agent Authentication

This security functionality ensures the TOE, when delivered to the Personalisation Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm.

SF.AA Active Authentication

This security functionality ensures the Active Authentication is performed as described in [R2] (if it is activated by the Personalisation Agent). A self-test on the random generator is performed prior to any Active Authentication. Moreover, this security functionality is protected against the DFA.

SF.SELFTESTS Self tests

The TOE performs self tests on the TSF data it stores to protect the TOE. In particular, it is in charge of the:

- DFA detection for the Active Authentication,
- Self tests of the random generator before the PACEV2 and Active Authentication,
- Self tests of the DES before the PACEV2,
- Monitoring of the integrity of keys, files and TSF data,
- Monitoring the integrity of the optional code (at start up),
- Protecting the cryptographic operation.

The integrity of the files are monitored each time they are accessed and the integrity of the optional code is checked each time the TOE is powered on.

The integrity of keys and sensitive data is checked each time they are used/accessed.

SF.SAFE_STATE_MGT Safe state management

This security functionalities ensures that the TOE gets back to a secure state when an integrity error is detected by F.SELFTESTS, a tearing occurs (during a copy of data in EEPROM).

This security functionality ensures that such a case occurs, the TOE is either switched in the state "kill card" or becomes mute.

SF.PHYSICAL_PROTECTION Physical protection

This security functionality protects the TOE against physical attacks.

SF.PREPERSONALISATION Prepersonalisation

This function is in charge of pre-initializing the product and loading patch code if needed.

7.2 Link between the TSF and SFR

	SF.ACC_READ	SF.ACC_WRITE	SF.EAC	SF.SM	SF.AUTH_PERSO	SF.AA	SF.SELFTESTS	SF.SAFE_STATE_MGT	SF.PHYSICAL_PROTECTION	SF.PREPERSONALISATION
FAU_SAS.1								X	X	
FCS_CKM.1/DH_PACEv2				X						
FCS_CKM.1/CA			X	X						
FCS_CKM.4			X	X						
FCS_COP.1/PACEv2_ENC	X			X						
FCS_COP.1/CA_ENC	X		X	X						
FCS_COP.1/PACEv2_MAC	X			X						
FCS_COP.1/CA_MAC	X		X	X						
FCS_COP.1/SIG_VER	X		X							
FCS_COP.1/AA	X					X				
FCS_RND.1			X	X	X	X	X			X
FIA_AFL.1/PACEv2	X									
FIA_UID.1/PACEv2	X		X	X						
FIA_UAU.1/PACEv2	X		X	X						
FIA_UAU.4/PACEv2	X		X	X						
FIA_UAU.5/PACEv2	X		X	X						
FIA_UAU.6/PACEv2	X									
FIA_UAU.6/EAC	X		X							
FIA_API.1	X		X							
FDP_ACC.1/TRM	X									
FDP_ACF.1/TRM	X		X	X						
FDP_RIP.1				X						
FDP_UCT.1/TRM	X	X								
FDP_UIT.1/TRM	X	X								
FMT_MOF.1/AA						X				
FMT_SMF.1		X			X			X		X
FMT_SMF.1/PP		X								X
FMT_SMR.1/PACEv2	X							X		

	SF.ACC_READ	SF.ACC_WRITE	SF.EAC	SF.SM	SF.AUTH_PERSO	SF.AA	SF.SELFTESTS	SF.SAFE_STATE_MGT	SF.PHYSICAL_PROTECTION	SF.PREPERSONALISATION
FMT_LIM.1								X	X	
FMT_LIM.2								X	X	
FMT_MTD.1/INI_ENA		X			X					X
FMT_MTD.1/INI_DIS	X									
FMT_MTD.1/CVCA_INI		X								
FMT_MTD.1/CVCA_UPD		X	X							
FMT_MTD.1/DATE		X	X							
FMT_MTD.1/CAPK		X								
FMT_MTD.1/PA		X								
FMT_MTD.1/KEY_READ	X									
FMT_MTD.3	X		X							
FPT_EMS.1			X		X	X				X
FPT_TST.1							X			
FPT_FLS.1 *								X		
FPT_PHP.3									X	
FTP_ITC.1/PACEv2	X			X						
FDP_DAU.1/AA						X				
FDP_ITC.1/AA		X				X				
FCS_CKM.1/AA						X				
FDP_ACC.2/PP										X
FDP_ACF.1/PP					X					X
FIA_UAU.1/PP										x
FIA_UID.1/PP										x
FCS_COP.1/PP					X					x
FTP_ITC.1/PP										X
FDP_UIT.1/PP										X
FDP_ITC.1/PP										X
FCS_CKM.1/PP					X					X
FDP_UCT.1/PP										X
FMT_MOF.1/PP										x

	SF.ACC_READ	SF.ACC_WRITE	SF.EAC	SF.SM	SF.AUTH_PERSO	SF.AA	SF.SELFTESTS	SF.SAFE_STATE_MGT	SF.PHYSICAL_PROTECTION	SF.PREPERSONALISATION
FCS_CKM.4/PP										**X**
FAU_STG.2								**X**		
FIA_AFL.1/PP					**X**					
FMT_MSA.1/PP										**X**
FMT_MSA.1/SM	**X**		**X**	**X**						
FMT_MSA.3/SM	**X**		**X**	**X**						

8 References

Travel Document specifications

[R1] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[R2] International Civil Aviation Organization, ICAO MACHINE READABLE Travel Documents, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[R3] 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

[R4] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization (this includes the latest supplemental for ICAO Doc 9303 which also should be considered).

[R5] Development of a logical data structure – LDS for optional capacity expansion technologies Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision – 1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

Common Criteria Protection Profiles

[R6] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0035 15/06/2007

[R7] Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, version 1.0, 2nd November 2011

[R8] Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, version 1.3.2

[R9] Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009

[R10] Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-2009, Version 1.10, 25th March 2009

[R11] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009

Security Target

[R12] NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cc081VIA Security Target Lite, BSI-DSZ-0555, Rev. 1.3, 21 September 2009

Standards

[R13] ISO7816-4 – Organization, security and commands for interchange

[R14] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009

[R15] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[R16] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[R17] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[R18] ISO/IEC 9796-2 (2002) - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[R19] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[R20] Federal Information Processing Standards Publication 180-2 Secure Hash Standard (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[R21] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[R22] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. RFC 3447, 2003

[R23] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002

[R24] ANSI X9.31 - Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[R25] FIPS 46-3 Data Encryption Standard (DES)

[R26] ISO/IEC 9797-1:1999 "Codes d'authentification de message (MAC) Partie 1: Mécanismes utilisant un cryptogramme bloc"

[R27] NIST SP 800-90 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)

[R28] FIPS 197 – Advance Encryption Standard (AES)

Misc

[R29] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R30] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

[R31] NOTE-06 – Patch Loading – draft version – ANSSI

CC

[R32] Common Criteria for Information Technology security Evaluation Part 1 : Introduction and general model, CCMB-2012-09-001, version 3.1 Revision 4, September 2012

[R33] Common Criteria for Information Technology security Evaluation Part 2 : Security Functional Components, CCMB-2012-09-002, version 3.1 Revision 4, September 2012

[R34] Common Criteria for Information Technology security Evaluation Part 3 : Security Assurance Components, CCMB-2012-09-003, version 3.1 Revision 4, September 2012

[R35] Référentiel general de sécurité, version 1.0 du 06/05/12

Oberthur Technologies

[R36] TARANIS Administration and Personalisation Guidance Document, FQR 110 6450 Ed1

9 Acronyms

AA	Active Authentication
BAC	Basic Access Control
CC	Common Criteria
CPLC	Card personalisation life cycle
DF	Dedicated File
DFA	Differential Fault Analysis
DG	Data Group
EAL	Evaluation Assurance Level
EF	Elementary File
EFID	File Identifier
DES	Digital encryption standard
DH	Diffie Hellmann
I/0	Input/Output
IC	Integrated Circuit
ICAO	International Civil Aviation organization
ICC	Integrated Circuit Card
IFD	Interface device
LDS	Logical Data structure
MF	Master File
MRTD	Machine readable Travel Document
MRZ	Machine readable Zone
MSK	Manufacturer Secret Key
OS	Operating System
PACEV2	Password Authenticated Connection Establishment version 2
PKI	Public Key Infrastructure
PP	Protection Profile
SFI	Short File identifier
SHA	Secure hashing Algorithm
SOD	Security object Data
TOE	Target of Evaluation
TSF	TOE Security function

Index

S

T

U