the security technology provider

http://www.gepitalia.it   *http://www.security.arjowiggins.com*

Arjowiggins Security SAS - Gep S.p.A.
via Remo De Feo, 1
80022 Arzano (NA), ITALY

Security Target

SOMA-c003 Electronic Passport EAC-SAC-AA

Public Version

Common Criteria version 3.1 revision 4
Assurance Level EAL 4+

Version	1.0
Date	2014-04-02
Reference	TCAE140024
Classification	PUBLIC

Version control

Version	Date	Author	Revision Description
1.0	2014-04-02	Marco EVANGELISTA	First version

Table of Contents

List of Tables

List of Figures

Abbreviations and Notations

Numerical values
Numbers are printed in decimal, hexadecimal or binary notation.
Hexadecimal values are indicated with a 'h' suffix as in XXh, where X is a hexadecimal digit from 0 to F.
Decimal values have no suffix.

Example: the decimal value 179 may be noted as the hexadecimal value B3h.

Denoted text
The text added to provide details on how the TOE implementation fulfils some security requirements is written in *italics* and is preceded by the numbered tag "Application Note".

Refinements to the security requirements are denoted by the tag "Refinement" and are written in **bold** text.

Selections and *assignments* made by the Protection Profile authors are written in <u>underlined</u> text.

Selections and *assignments* made by the authors of this ST are written in <u>**underlined bold**</u> text.

Iterations are denoted by showing a slash "/", and the iteration indicator after the component indicator.

The original text of the selection and assignment components, as defined by the Common Criteria, is given by a footnote.

Key words
The words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" are to be interpreted as described in RFC2119 [R22].

1.   Introduction

1.1   ST Overview

This Security Target (ST) document defines the security objectives and requirements, as well as the scope of the Common Criteria evaluation, of the SOMA-c003 electronic passport.

The Target Of Evaluation (TOE) is the contactless integrated circuit chip STMicroelectronics ST23R160/80A/48A revision B, programmed with the operating system and with the passport application, according to ICAO Doc 9303 [R18].

In this ST, the term ST23R160/80A/48A means the master product ST23R160, and two commercial derivatives: ST23R80A and ST23R48A. The three ICs only differ in the EEPROM size.

The TOE adds security features to a passport booklet, providing machine-assisted identity confirmation and machine-assisted verification of document security.

This ST addresses the following advanced security methods:
- Extended Access Control (EAC) v1, according to the BSI technical guideline TR-03110 v2.10 [R8] which includes Chip Authentication and Terminal Authentication,
- Supplemental Access Control (SAC), according to ICAO TR-SAC [R20] and
- Active Authentication according to ICAO Doc 9303 part 3 vol. 2 [R18].

The TOE also supports Basic Access Control (BAC), according to ICAO Doc 9303 [R18], which is addressed by an other ST [R14].

1.2   ST reference

Table 1-1   ST Identification

Title	Security Target SOMA-c003 Electronic Passport EAC-SAC-AA – Public Version
Version	1.0
Author	Marco EVANGELISTA
Reference	TCAE140024
Keywords	Security target, security target lite, common criteria

1.3   TOE reference

Table 1-2   TOE Identification

Product Name	SOMA-c003
Product Version	1.2
TOE Identification Data	53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 33h 5Fh 31h 5Fh 32h
Evaluation Criteria	Common Criteria version 3.1 revision 4
Protection Profiles	BSI-CC-PP-0056-V2-2012 v1.3.2 BSI-CC-PP-0068-V2-2011 v1.0
Evaluation Assurance Level	EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
Developer	Arjowiggins Security SAS - Gep S.p.A.
Evaluation Sponsor	Arjowiggins Security SAS - Gep S.p.A.
Evaluation Facility	SERMA Technologies' ITSEF
Certification Body	ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information
Certification ID	SOMA-c003
Keywords	electronic passport, e-Passport, MRTD, Machine Readable Travel Document, ICAO, Extended Access control, EAC, Password Authenticated Connection Establishment (PACE), Supplemental Access Control (SAC), Active Authentication

The TOE is delivered as a chip ready for pre-personalization. It is identified by the following string, representing the Global Reference:

SOMA-c003_1_2
(ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 33h 5Fh 31h 5Fh 32h)

The last three bytes encode the OS version as follows:
- Byte 11 encode the ROM code version: 1 (ASCII code 31h)
- Byte 12 is a field separator
- Byte 13 encode the Patch version: 2 (ASCII code 32h)

Application Note 1:   *The OS version is composed of a major version number, indicating the ROM code version, and of a minor version number, indicating the patch version. The major version number and the minor version number are separated by the character "_" (underscore, ASCII code 5Fh). A minor version number 0 (ASCII code 30h) indicates that no patch is loaded.*

The TOE identification data are located in the non-volatile memory of the chip. Instructions for reading identification data are provided by the guidance documentation.

1.4   TOE overview

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by this ST is an electronic travel document representing a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [R20] (which means amongst others according to the Logical Data Structure (LDS) defined in [R18]) and additionally providing the Extended Access Control according to the BSI TR-03110 [R8], and the Active Authentication according to the ICAO Doc 9303 [R18].

The TOE also features the Basic Access Control (BAC) mechanism, according to the ICAO Doc 9303 [R18], which is addressed by an other ST [R14].

The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [R7].
The TOE is composed of:
- the circuitry of the MRTD's chip ST23R160/80A/48A (see Appendix A),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (SOMA-c003 Operating System),
- the *ePassport application* and
- the associated guidance documentation [R15][R16][R17].

On account of its composite nature, the TOE evaluation builds on the evaluation of the integrated circuit.

The TOE is connected to an antenna for wireless communication. Both the TOE and the antenna are embedded in a paper or plastic substrate, that provides mechanical support and protection. The resulting device (TOE, antenna and substrate), is called "inlay" as it is intended to be inserted in a passport booklet (see section 1.4.3.2).
Once personalized with the data of the legitimate holder and with security data, the e-Passport can be inspected by authorized agents.

1.4.2 TOE Usage and security features for operational use

A State or Organization issues travel documents to be used by the holder for international travel. The traveler presents a travel document to the inspection system to prove his or her identity.

The travel document in context of this security target contains:
  i.   visual (eye readable) biographical data and portrait of the holder,
  ii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
  iii. data elements on the travel document's chip according to LDS for contactless machine reading.

The authentication of the traveler is based on:

- the possession of a valid travel document personalized for the traveller 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 Organization ensures the authenticity of the data of genuine travel documents. The receiving state trusts a genuine travel document of an Issuing State or Organization.

For this security target the travel document is viewed as the 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:
  - i. the biographical data on the biographical data page of the data travel surface,
  - ii. the printed data in the Machine-Readable Zone (MRZ),
  - iii. the printed portrait
- the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [R12] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the travel document holder:
  - i. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  - ii. the digitized portraits (EF.DG2),
  - iii. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1];
  - iv. the other data according to LDS (EF.DG5 to EF.DG16),
  - v. the Document security object (SO_D) and
  - vi. security data objects required for product management.

The Issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and its data. The physical part of the travel document as the travel document's chip are uniquely 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 organizational security measures (e.g. control of materials, personalization procedures) [R18]. These security measures can include the binding of the travel documents chip to the travel document.

The logical travel documents delivered by the IC Manufacturer to the Travel Document Manufacturer is protected by a mutual authentication mechanism based on symmetric cryptography with diversified key, until completion of the initialization and pre-personalization processes. After completion the authentication keys are disabled.

---

[1] These biometric reference data are optional according to [R18]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

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 required security methods Passive Authentication and the following 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 an optional security measure in the ICAO Doc9303 [R18] and
- Password Authenticated Connection Establishment [R20].

The Passive Authentication mechanism is performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical travel document:
  i. in integrity by write-only-once access control and by physical means and
  ii. in confidentiality by the Extended Access Control Mechanism.

As BAC is also supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [R5] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

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

For the PACE protocol according to [R20], the following steps shall be performed:
  i. The travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal
  ii. The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
  iii. The travel document's chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.
  iv. Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [R7][R20].

This security target requires the TOE to implement the Extended Access Control as defined in [R7] and additionally the Active Authentication as defined in [R18]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal authentication v.1 to protect the

confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated 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.

The Active Authentication authenticates the travel document to the inspection system.

1.4.3 TOE Life-cycle

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

1. Development, composed of (i) the development of the operating system software by the Embedded Software Developer and (ii) the development of the integrated circuit by the IC Manufacturer
2. Manufacturing, composed of (i) the fabrication of the integrated circuit by the IC Manufacturer, (ii) the embedding of the chip in an inlay with an antenna, (iii) the completion of the operating system, (iv) the initialization and pre-personalization of the MRTD
3. Personalization
4. Operational Use

Application Note 2:   *The entire Development phase, as well as step (i) "fabrication of the integrated circuit" of the Manufacturing phase are the only phases covered by assurance as during these phases the TOE is under construction in a protected environment.*

With respect to the [R4], the TOE life-cycle is additionally subdivided into 7 steps.

In Figure 1-1 activities (rounded rectangles) and deliveries (arrows) printed orange are secured by the environment and are covered by assurance class ALC. The ones printed white refer to phases covered by assurance class AGD, in which the TOE is self-protected.

Figure 1-1   TOE life-cycle

Phase 1 – Development

Step 2 — Embedded software development — AWS-Gep

Step 1 — IC design and dedicated software development

Step 3 — Integration → Mask fabrication

ST Micro electronics

Phase 2 - Manufacturing

IC manufacturing

TOE delivery

TOE under consruction in a secured enviroment

Step 4 — Inlay Manufacturing → Assembling of the book

Step 5 — Pre-personalization

Travel document Manufacturer

Phase 3 - Personalization

Step 6 — Personalization

Personalization Agent

Phase 4 – Operational Use

Step 7 — Operational use → End of life

Travel document Holder/ Inspection system

Delivered self-protected TOE

Table 1-3 identifies the roles in each phase of the TOE life cycle.

Table 1-3   Roles Identification

Phase	Role	Identification
1	IC Developer	STMicroelectronics
1	Embedded Software Developer	Arjowiggins Security SAS - Gep S.p.A.
2	IC Manufacturer	STMicroelectronics
2	Travel document Manufacturer	the agent who is acting on the behalf of the Issuing State or Organization to assemble the passport book embedding the TOE, and to pre-personalize the MRTD
3	Personalization Agent	the agent who is acting on the behalf of the Issuing State or Organization to personalize the MRTD for the holder
4	Travel document Holder	The rightful owner of the MRTD

1.4.3.1   Phase 1   "Development"

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

Step2 "Embedded Software Development"
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 ePassport 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 ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

1.4.3.2   Phase 2   "Manufacturing"

Step3 "IC Manufacturing"
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

(i)   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.

(ii)   Creates the ePassport application

Application Note 3: *Creation of the application implies the creation of MF and ICAO.DF*

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).

Step4 (optional) "Travel document manufacturing – Assembling of the book"
The travel document manufacturer combines the IC with hardware for the contactless interface in the travel document unless the travel document consists of the card only.

Step5 "Travel document manufacturing – Pre-Personalization"
The travel document manufacturer equips travel document's chips with pre-personalization Data.

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

1.4.3.3   Phase 3   "Personalization of the MRTD"

Step6 "Personalization"
The personalization 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 Personalization Agent and includes but is not limited to the creation of
  (i)   the digital MRZ data (EF.DG1),
  (ii)   the digitized portrait (EF.DG2), and
  (iii)   the Document security object.

The signing of the Document security object by the Document signer[R18] finalizes the personalization of the genuine travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application Note 4: *The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [R10], section 92) comprise (but are not limited to) the Personalization Agent Key(s) and the Chip Authentication Private Key.*

Application Note 5:   *This security target distinguishes between the Personalization Agent as an entity known to the TOE and the Document Signer as an entity in the TOE IT environment signing the Document security object as described in [R18]. This approach allows but does not enforce the separation of these roles.*

1.4.3.4   Phase 4   "Operational Use"

Step7 "Operational Use"
The TOE is used as 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 Organization and can be used according to the security policy of the issuing State, but they can never be modified.

Application Note 6:   *This ST considers the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore defines the TOE delivery according to CC after Step 3 of phase 2. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has too be taken by the certification body resp. the national body of the issuing State or Organisation. In this case the national body of the issuing State or Organisation is responsible for these specific production steps.*
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" (pahse 4) have to be considered in the product evaluation process under AGD assurance class. Therefore this security target outlines 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.

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

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

1.5   TOE Description

1.5.1 Physical scope of the TOE

The physical TOE is composed of the following:
- the integrated circuit chip ST23R160/80A/48A (microcontroller) programmed with the operating system and with the passport application.

The microcontroller ST23R160/80A/48A on which the SOMA-c003 operating system builds is described in Appendix A.

1.5.2 Other non-TOE physical components

The antenna and the substrate of the inlay are not part of the TOE.
Figure 1-2 shows the inlay components, distinguishing between TOE components and non-TOE components.

Figure 1-2   Inlay components
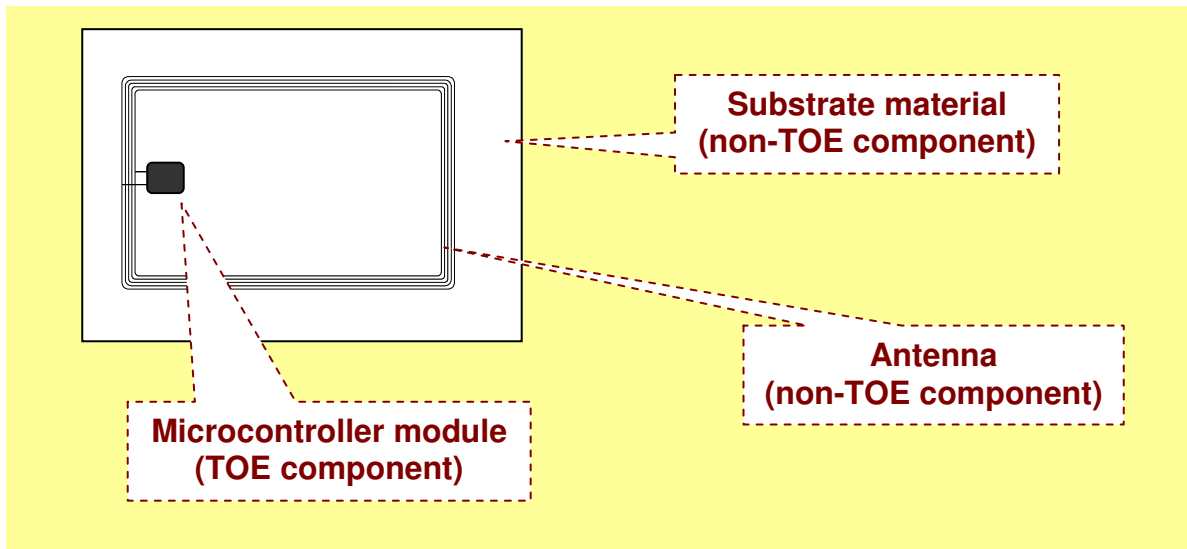
1.5.3 Logical scope of the TOE

The logical part of the TOE comprises the following software components stored in the non-volatile memory units of the microcontroller:

- operating system
- file system
- ePassport application
- security data objects

The SOMA-c003 operating system manages all the resources of the integrated circuit that equips the passport, providing secure access to data and functions. Major tasks performed by the operating system are:

- Communication between internal objects
- Communication with external devices
- Data storage in the file system
- Execution of commands
- Cryptographic operations
- Management of the security policies

The operating system has a flexible modular structure and a layered architecture featuring:

- full support of the ICAO ePassport application
- Basic Access Control
- Extended Access Control
- Supplemental Access Control
- Active Authentication
- secure support of various types of applications
- secure management of functions and data

The file system contains security data objects and the ePassport application.

During Initialization, the IC Manufacturer stores, among other data, the product identification data and the travel document Manufacturer keys. After the Initialization, access to the resource of the delivered TOE is protected by a symmetric cryptographic mechanism requiring a mutual authentication.

In the pre-personalization phase, the travel document Manufacturer stores, among other data, the Personalization Agent keys, the Chip Authentication keys (public key in EF.DG14), the Active Authentication keys (public key in EF.DG15) and the EF.CardAccess (according to [R20]).

In the personalization phase, the Personalization Agent writes, among other data, the elementary files of the LDS (DG1 to DG13, DG16, EF.COM, and EF.SOD), as well as the keys for BAC and SAC mechanisms, the Certificate Authority References (stored in EF.CVCA), the initial CVCA certificate reference (the trustpoint) and the date of its generation.

Once the passport is in the Operational state, no data can be deleted or modified, except for the current date, the trustpoint and the EF.CVCA file which can also be modified.

2.   Conformance claims

2.1   Common Criteria Conformance Claim

This Security Target claims conformance to:

- Common Criteria version 3.1 revision 4, International English Version [R10][R11][R12], as follows:
    o Part 2 (security functional requirements) extended
    o Part 3 (security assurance requirements) conformant

The software part of the TOE runs on the chip STMicroelectronics ST23R160/80A/48A (see Appendix A). This integrated circuit is certified against Common Criteria at the assurance level EAL6+ (cf. Appendix A).

2.2   Protection Profile Conformance Claim

This ST claims strict conformance to:
- BSI-CC-PP-0056-V2-2012 Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2 05th December 2012 [R6].

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

2.3   Package Conformance Claim

This Security Target claims conformance to:

- EAL4 assurance package augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 defined in the CC part 3 [R12]

2.4   Conformance Claim Rationale

This ST claims conformance to the PACE PP [R7] and EAC PP [R6]. The parts of the TOE listed in those Protection Profiles correspond to the ones listed in section 1.4.1 of this ST.

In this ST, the TOE will be delivered from the IC Manufacturer to the Travel document Manufacturer after Step3 "IC Manufacturing" of Phase 2, as a chip, in accordance with Application Note 4 of the EAC PP [R6]. At TOE delivery, there is no user data or machine readable data available. The EF.DG14 and EF.DG15 files, containing part of the user data, are written by the Travel Document Manufacturer in Step5 "MRTD Manufacturing – Pre-Personalization" of Phase 2. The remaining user data as well as applicative files are written by the Personalization Agent, during Phase 3 "Personalization of the MRTD".

The security problem definition includes the assets, the subjects, the assumptions, the threats and the organisational security policies of both PPs.

Table 2-1 specifies the source (PACE PP or EAC PP) of assumptions, threats and organisational security policies.

Table 2-1   Source of assumptions, threats and OSPs

	Source	
	PACE PP [R7]	**EAC PP [R6]**
Assumptions	• A.Passive_Auth	• A.Ins_Sys • A.Auth_PKI
Threats	• T.Skimming • T.Eavesdropping • T.Tracing • T.Forgery • T.Abuse-Func • T.Information_Leakage • T.Phys-Tamper • T.Malfunction	• T.Read_Sensitive_Data • T.Counterfeit
Organisational Security Policies	• P.Manufact • P.Pre-Operational • P.Card_PKI • P.Trustworthy_PKI • P.Terminal	• P.Sensitive_Data • P.Personalisation

The security objectives of both PPs are included in this ST.
Table 2-2 specifies the source (PACE PP or EAC PP) of security objectives for the TOE and of security objectives for the operational environment.

Table 2-2   Source of security objectives

	Source	
	PACE PP [R7]	**EAC PP [R6]**
Security Objectives for the TOE	• OT.Data_Integrity • OT.Data_Authenticity • OT.Data_Confidentiality • OT.Tracing • OT.Prot_Abuse-Func • OT.Prot_Inf_Leak • OT.Prot_Phys-Tamper • OT.Prot_Malfunction • OT.Identification • OT.OT.AC_Pers	• OT.Sens_Data_Conf • OT.Chip_Aut_Proof
Security Objectives for the operational environment	• OE.OE.Personalisation • OE-Passive_Auth_Sign • OE.Terminal • OE.Travel_Document_Holder • OE.Legislative_Compliance	• OE.Chip_Auth_Key_Travel_Document • OE.Active_Auth_Key_Travel_Document • OE.Authoriz_Sens_Data • OE.Exam_Travel_Document • OE.Prot_Logical_Travel_Document • OE.Ext_Insp_Systems

Note that the objective named OE.Auth_Key_Travel_Document in the EAC PP has been renamed to OE.Chip_Auth_Key_Travel_Document to distinguish it from the similar objective that has been added to this ST to cover the Active Authentication (see Table 2-3 below).

Table 2-3 lists the security objectives that have been added to this ST to cover the Active Authentication mechanism.

Table 2-3   Added security objectives

Security Objective	Definition	Operation
OT.Active_Auth_Proof	Proof of travel document's chip authenticity by Active Authentication	Addtion covering the proof of IC authenticity for Basic Inspection Systems
OE.Active_Auth_Key_Travel_Document	Travel document Active Authentication key	Addition covering the generation, signature and storage of the Active Authentication key pair, as well as the support to the Inspection System.

The functional requirements described in section 6 of this ST include the SFRs of both the PACE PP [R7] and EAC PP [R6].
Table 2-4 specifies the source (PACE PP or EAC PP) of security functional requirements.

Table 2-4   Source of Security Functional Requirements

	Source	
	PACE PP [R7]	**EAC PP [R6]**
SFRs	• FCS_CKM.1/DH_PACE • FCS_CKM.4 • FCS_COP.1/PACE_ENC • FCS_COP.1/PACE_MAC • FCS_RND.1 • FIA_AFL.1/PACE • FIA_UID.1/PACE • FIA_UAU.1/PACE • FIA_UAU.4/PACE • FIA_UAU.5/PACE • FIA_UAU.6/PACE • FDP_ACC.1/TRM • FDP_ACF.1/TRM • FDP_RIP.1 • FDP_UCT.1/TRM • FDP_UIT.1/TRM • FDP_ITC.1/PACE • FAU_SAS.1 • FMT_SMF.1 • FMT_SMR.1/PACE • FMT_LIM.1 • FMT_LIM.2 • FMT_MTD.1/INI_ENA • FMT_MTD.1/INI_DIS • FMT_MTD.1/KEY_READ • FMT_MTD.1/PA • FPT_EMS.1 • FPT_FLS.1 • FPT_TST.1 • FPT_PHP.3	• FCS_CKM.1/CA • FCS_COP.1/CA_ENC • FCS_COP.1/SIG_VER • FCS_COP.1/CA_MAC • **FIA_UID.1/PACE** • **FIA_UAU.1/PACE** • **FIA_UAU.4/PACE** • **FIA_UAU.5/PACE** • **FIA_UAU.6/PACE** • FIA_UAU.6/EAC • <u>FIA_API.1/CA</u> • **FDP_ACC.1/TRM** • **FDP_ACF.1/TRM** • **FMT_SMR.1/PACE** • **FMT_LIM.1** • **FMT_LIM.2** • FMT_MTD.1/CVCA_INI • FMT_MTD.1/CVCA_UPD • FMT_MTD.1/DATE • FMT_MTD.1/CAPK • **FMT_MTD.1/KEY_READ** • FMT_MTD.3 • **FPT_EMS.1**

In the above table, note the following points:
- The EAC PP SFRs written in bold text cover the definition in PACE PP and extend them for EAC. These extensions do not conflict with strict conformance to PACE PP.
- An iteration label has been added to the EAC PP SFRs printed in underlined text, to distinguish them from the similar SFRs that have been added to this ST (see Table 2-5 below). The requirement definitions remain unchanged with respect to the PP.

Iterations and changes to the SFRs, with respect to PACE PP and EAC PP, are listed in Table 2-5. These changes do not lower TOE security.

Table 2-5   Additions, iterations and changes to SFRs

Security Functional Requirement	Operation
FIA_API.1/AA	**Iteration** This iteration has been added to cover the proof of identity by means of Active Authentication.
FIA_API.1/CA	**Iteration** An iteration label has been added to the FIA_API.1 SFR in EAC PP, to distinguish it from the FIA_API.1/AA SFR added to this ST. The requirement definition remains unchanged.
FCS_COP.1/AA_SIGN	**Iteration** This iteration has been added to cover the signature of Active Authentication data.
FMT_MTD.1/AAPK	**Iteration** This iteration has been added to restrict the ability to write the Active Authentication private key
FMT_MTD.1/ADDTSF_WRITE Management of TSF data – additional TSF data write	**Iteration** This iteration has been added to cover the storage of additional TSF data in personalization
FIA_UAU.4/PACE Single use authentication mechanisms – single use authentication of the Terminal by the TOE	**Change of Application Note** The application note now clarifies that this SFR also relates to the Travel Document Manufacturer authentication (cf. Application Note 54:).
FIA_UAU.5/PACE Multiple authentication mechanisms	**Change of definition** the Travel Document Manufacturer has been added as a user allowed to authenticate to the passport (cf. Application Note 56:).

3.   Security Problem Definition

3.1   Introduction

Application Note 7:   *With respect to the security problem definition defined in the protection profiles, this ST has some additions concerning the Active Authentication.*

3.1.1 Assets

Due to strict conformance to both EAC PP [R6] and PACE PP [R7], this ST includes, as assets to be protected, all assets listed in section 3.1 of those PPs.

3.1.1.1   Assets to be protected according to PACE PP

The primary assets to be protected by the TOE as long as they are in scope of the TOE are listed in Table 3-1 (please refer to the glossary in chap. 7 for the term definitions).

Table 3-1   Primary assets

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
travel document			
1	User data stored on the TOE	All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [R20] and being allowed to read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R20]). This asset covers "User Data on the MRTD's chip", "Logical MRTD Data" and "sensitive User Data" in [R5].	Confidentiality[2] Integrity Authenticity

---

[2] Though note ac data element stored on the TOE represents a secret, the specification [R20] anyway requires securing their confidentiality: only terminals authenticated according to [R20] can get access to the user data stored. They have to be operated according to P.Terminal.

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
2	User data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [R20] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R20]). User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality[3] Integrity Authenticity
3	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 PACE password. TOE tracing data can be provided/gathered.	unavailability[4]

Application Note 8:   *Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current PP also secures these specific travel document holder's data as stated in the table above.*

All these primary assets represent User Data in the sense of CC.

The secondary assests also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

---

[3] Though not each data element being transferred represents a secret,, the specification [R20] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [R20].

[4] Represents a prerequisite for anonymity of the travel document holder

Table 3-2 Secondary assets

Object No.	Asset	Definition	Property to be maintained by the current security policy
travel document			
4	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.	Availability
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers "Authenticity of the MRTD's chip" in [R5].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other on-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	Travel document communication establishment authorisation data	Restricted-revealable[5] authorisatin information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be sent to it.	Confidentiality Integrity

Application Note 9:   *Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.*

Application Note 10:   *Travel document communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored*

---

[5] The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.

in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt.

The TOE shall secure the reference information as well as – together with the terminal connected[6] - the verification information in the "TOE ⇔ terminal" channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be sent to the TOE.

The secondary assets represent TSF and TSF-data in the sense of CC.

3.1.1.2   Assets to be protected according to EAC PP

Logical travel document sensitive User Data

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

Application Note 11: *Due to interoperability reasons the "ICAO Doc 9303" [R18] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode according to this ST, if it is accessed using BAC [R18] (conformance to the BAC certification [R14] is kept, though). Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [R5]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to potential attacks.*

A sensitive asset is the following more general one.

Authenticity of the travel document's chip

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

3.1.2 Subjects

This security target considers the subjects defined in the PACE PP, and in the EAC PP. The subjects considered in accordance with the PACE PP are listed in Table 3-3.

Table 3-3   Subjects and external entities according to PACE PP

External Entity No.	Subject No.	Role	Definition
1	1	Travel document holder	A person for whom the travel document Issuer has personalised the travel document[7]. This entity is commensurate with MRTD Holder in [R5].Please note that a travel document holder can also be an attacker (s. below).

---

[6] The travel document holder mayreveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.

External Entity No.	Subject No.	Role	Definition
2	-	Travel document presenter (traveller)	A person presenting the travel document to a terminal[8] and claiming the identity of the travel document holder. This external entity is commensurate with "Traveller" in [R5]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role "Termninal" 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 [R5].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspection authority[9] and verifiying 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.
5	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [R18]. This role is usually delegated to a Personalization Agent.

---

[7] i.e. this person is uniquely associated with a concrete electronic Passport
[8] In the sense of [R20]
[9] Concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
6	-	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 (C_{CSCA}) having to e distributed by strictly secure diplomatic means, see [R18], 5.5.1.
7	4	Personalizati on Agent	An organization 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, (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 [R18], (iv) writing the document details data, (v) writing the initial TSF data data, (vi) signing the Document Security Object defined in [R18] (in the role fo DS). Please note that the role "Personalisation Agent" may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with "Personalization Agent" in [R5].
8	5	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[10]. The TOE itself does not distinguish between the IC Manufacturer and the travel document Manufacturer using this role Manufacturer. This entity commensurate with "Manufacturer" in [R5].

---

[10] Cf. also sec. 1.4.3 above

External Entity No.	Subject No.	Role	Definition
9	-	Attacker	A thereat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might "capture" any subject role recognised by the TOE. This external entity is commensurate to "Attacker" in [R5].

Application Note 12: *The subject "Basic Inspection System with BAC" (BIS-BAC) is described in an other ST [R14].*

In addition to the subjects defined by the PACE PP, this ST considers the following subjects defined by the EAC PP:

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

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

- **Terminal**: A terminal is any technical system communicating with the TOE through the contactless interface.

- **Inspection system (IS)**: A technical system used by the border control officer of the receiving State (i) in 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 (see Figure 3-1) and therefore (i) contains a terminal for the with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [R8] and (v) is authorized by the issuing State or

Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

- **Attacker**: Additionally to the definition in Table 3-3, the definition of an attacker is refined as follows: A threat agent trying (i) to manipulate the logical travel document without authorisation, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (ii) to forge a genuine travel document, or (iv) to trace a travel document.

Application Note 13: *An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.*

Figure 3-1   Advanced Inspection Procedure
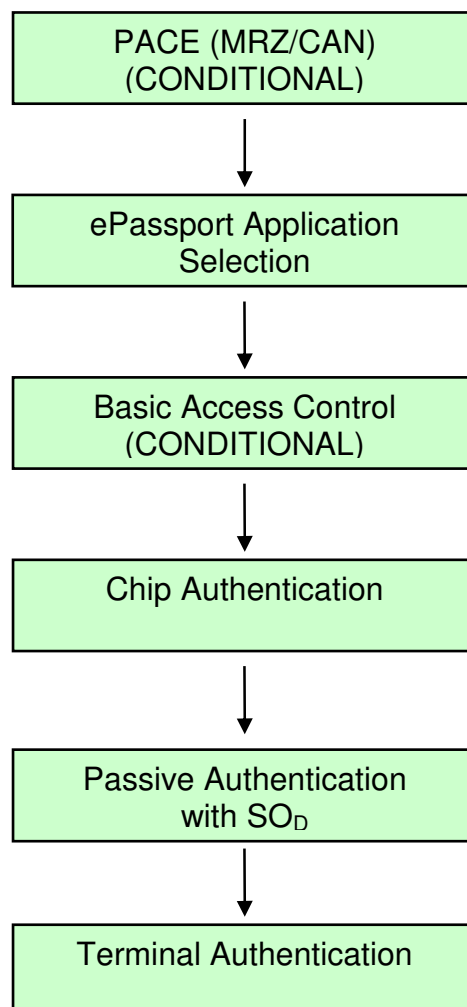
3.2 Assumptions

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

- **A.Passive_Auth** **PKI for Passive Authentication**

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical 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 and distributes them to the receiving States and Organizations. It is assumed that the Document Security Object contains only the hash values of the genuine user data according to [R18].

- **A.Insp_Sys** **Inspection Systems for global interoperability**

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [R20] and/or BAC [R5]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [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** **PKI for Inspection Systems**

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the

public keys of their Country Verifying Certification Authority to their travel document's chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [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.

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.Skimming   Skimming   travel   document/Capturing   Card-Terminal Communication**

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

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

    Asset: confidentiality of logical travel document data

Application Note 14: *A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.*

Application Note 15: *MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Trave_Document_Holder.*

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

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

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

    Asset: confidentiality of logical travel document data

Application Note 16: *A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.*

- **T.Tracing**   **Tracing travel document**

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

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

Asset: privacy of the travel document holder

Application Note 17: *This threat completely covers and extends "T.Chip-ID" from BAC PP* [R5].

Application Note 18: *A product using BAC (whatever the type of the inspection system is: BIS_BAC) cannot avert this threat in the context of the security policy defined in this ST.*

Application Note 19: *Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a threat like T.Counterfait (counterfeiting travel document)[11] cannot be averted by the current TOE.*

- **T.Forgery**   **Forgery of data**

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

Threat agent: having high attack potential

Asset: integrity of the travel document

The TOE shall avert the threat as specified below.

---

[11] Such a torea might be formulated like: "An attacker produces an unauthorised copy or reproduction of a genuine travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to initiate this genuine travel document. This violates the authenticity of the travel document being used for authentication of a travel document presenter as the travel document holder.

- **T.Abuse-Func   Abuse of Functionality**

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the *User Data stored in the TOE*, (ii) to manipulate or to disclose the *TSF-data stored in the TOE* or (iii) to manipulate (bypass, deactivate or modify) *soft-coded security functionality of the TOE*. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

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

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

Application Note 20:   *Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.*

- **T.Information_Leakage   Information Leakage from travel document**

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

Threat agent: having high attack potential

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

Application Note 21:   *Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).*

- **T.Phys_Tamper   Physical Tampering**

Adverse action: An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the

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

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

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

Application Note 22:　*Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.*

- **T.Malfunction**　　**Malfunction due to Environmental Stress**

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

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

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

Application Note 23:　*A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.*

- **T.Read_Sensitive_Data   Read the sensitive biometric reference data**

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming (cf. [R14]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical MRTD as well.

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

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

- **T.Counterfeit   Counterfeit of MRTD's chip**

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

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

Asset: authenticity of logical MRTD data

3.4   Organizational Security Policies

The TOE and/or its environment shall comply to the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

- **P.Manufact   Manufacturing of the travel document's chip**

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

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

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

2. The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the 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. <u>before</u> they are in the operational phase, cf. section. 1.4.3 above.

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

- **P.Card_PKI   PKI for Passive Authentication (issuing branch)**

Application Note 24:   *The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.*

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

2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [R18], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [R18], 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   Trustworthyness of PKI**

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

- **P.Terminal   Abilities and trustworthyness of terminals**

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

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [R18].

2. They shall implement the terminal parts of the PACE protocol [R20], of the Passive Authentication [R18] and use them in this order[12]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

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

4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [R18]).

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

- **P.Sensitive_Data   Privacy of sensitive biometric reference data**

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

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

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The

---

[12] This order is commensurate with [R20]

personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

4.   Security Objectives

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

4.1   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.Data_Integrity   Integrity of Data**

The TOE must ensure integrity of the User Data and the TSF-data[13] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

- **OT.Data_Authenticity   Authenticity of Data**

The TOE must ensure authenticity of the User Data and the TSF-data[14] stored on it by enabling verification of their authenticity at the terminal-side[15].The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[16]

- **OT.Data_Confidentiality   Confidentiality of Data**

The TOE must ensure confidentiality of the User Data and the TSF-data[17] by granting read access only to the PACE authenticated BIS-PACE connected.The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

- **OT.Tracing   Tracing travel document**

---

[13] Where appropriate, see Table 3-2 above
[14] Where appropriate, see Table 3-2 above
[15] Verification od SO_D
[16] Secure messaqging after PACE authentication, see also [R20]
[17] Where appropriate, see Table 3-2 above

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

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

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

- **OT.Prot_Inf_Leak   Protection against Information Leakage**

The TOE must provide protection against disclosure of confidential User Data and/or TSF-data stored and/or processed in 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 and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Application Note 25:   *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.*

- **OT.Prot_Phys-Tamper   Protection against Physical Tampering**

The TOE must provide protection of 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 representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between 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 functionality.

- **OT.Prot_Malfunction   Protection against Malfunctions**

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

conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment.*

- **OT.Identification   Identification of the TOE**

The TOE must provide means to store Initialisation[18] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

- **OT.AC_Pers   Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R18] and the TSF data can be written by authorized Personalization 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 personalization of the document.

Application Note 26:   *The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.*

- **OT.Sens_Data_Conf   Confidentiality of sensitive biometric reference data**

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

- **OT.Chip_Auth_Proof   Proof of travel document's chip authenticity**

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Chip Authentication Version 1 as defined in [R8]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

---

[18] Amongst other, IC identification data

Application Note 27: *The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [R18] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.*

The following Security Objective for the TOE is an addition to the objectives given by the Protection Profiles to cover the Active Authentication mechanism.

- **OT.Active_Auth_Proof   Proof of travel document's chip authenticity**

The TOE must support the Basic Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Active Authentication as defined in [R18]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

4.2   Security Objectives for the Operational Environment

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   Issuing of the travel document**

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

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 (see also the Application Note 23 above).

- **OE.Passive_Auth_Sign   Authentication of travel document by Signature**

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained.
A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the

Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [R18]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [R18]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

- **OE.Personalisation**   **Personalisation of travel document**

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [R18][19], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [R18] (in the role of a DS).

Terminal operator: Terminal's receiving branch

- **OE.Terminal**   **Terminal operating**

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [R18].

2. The related terminals implement the terminal parts of the PACE protocol [R20], of the Passive Authentication [R18] (by verification of the signature of the Document Security Object) and use them in this order[20]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

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

4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [R18]).

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

---

[19] See also [R18], sec. 10

[20] This order is commensurate with [R20]

Application Note 28:   OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [R5].

Travel document holder Obligations

- **OE.Travel_Document_Holder   Travel document holder Obligations**

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

Issuing State or Organization

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

- **OE.Chip_Auth_Key_Travel_Document   Travel document Authentication Key**

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Justification: This security objective for the operational environment is needed to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the features of the TOE described only in this Security Target.

- **OE.Authoriz_Sens_Data   Authorization for Use of Sensitive Biometric Reference Data**

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

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the features of the TOE described only in this Security Target.

The following Security Objective for the Operational Environment is an addition to the objectives given by the Protection Profiles to cover the Active Authentication mechanism.

- **OE.Active_Auth_Key_Travel_Document   Travel document Active Authentication key**

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

Receiving State or Organization

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

- **OE.Exam_Travel_Document   Examination of the physical part of the travel document**

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

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from above OE.Terminal and therefore also counters T.Forgery and A.Passive_Auth. This is done because this ST introduces the Extended Inspection System, which is needed to handle the features of a travel document with Extended Access Control.

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

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

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

- **OE.Ext_Insp_Systems   Authorization of Extended Inspection Systems**

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

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

4.3   Security Objective Rationale

Table 4-1 provides an overview for security objectives coverage.

Table 4-1   Security Objective Rationale

	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.Active_Auth_Proof	OT.OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Chip_Auth_Key_Travel_Document	OE.Active_Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Read_Sensitive_Data	X															X			X					
T.Counterfait		X	X											X	X	X								
T.Skimming					X	X	X																X	
T.Eavesdropping							X																	
T.Tracing								X															X	
T.Abuse-Func									X															
T.Information_Leakage										X														
T.Phys-Tamper												X												
T.Malfunction													X											
T.Forgery			X	X	X		X				X					X					X	X	X	
P.Sensitive_Data	X															X			X					
P.Personalization			X						X											X				
P.Manufact									X															
P.Pre-Operational			X						X											X				X
P.Terminal																	X					X		
P.Card_PKI																					X			
P.Trustworthy_PKI																					X			
A.Insp_Sys																	X	X						
A.Auth_PKI																X			X					
A.Passive_Auth																	X				X			

A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below.

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless/contact interface. This threat is countered by the security objectives OT.Data_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. The objective OE.Travel_Document_Holder ensures that a PACE session can only be

established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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

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

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

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

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

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

The OSP **P.Pre-Operational** is enforced by the following security objectives:OT.Identification is affine to the OSP's property 'traceability before the operational phase';OT.AC_Pers and OE.Personalisation together enforce the OSP's

properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents';OE.Legislative_Compliance is affine to the OSP's property 'compliance with laws and regulations'.

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

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

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

The OSP **P.Personalisation** "Personalisation of the travel document by issuing State or Organisation only" addresses the (i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** "Personalisation of logical travel document", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document". Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation Agent.

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

The OSP **P.Terminal** "Abilities and trustworthiness of terminals" is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [7]. **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** "Counterfeit of travel document chip data" addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is

thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Chip_Auth_Key_Travel_Document** "Travel document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip.

In addition, the threat **T.Counterfeit** "Counterfeit of travel document chip data" is countered by chip an identification and authenticity proof required by **OT.Active_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organisation. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** "Travel document Authentication Key".
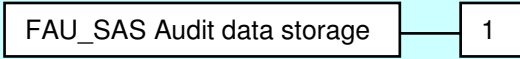
5.   Extended Components Definition

This ST uses components defined as extensions to CC part 2 [R11]. These components are drawn from PACE PP [R7] and from EAC PP [R6].

5.1   Definition of the family FAU_SAS

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

Table 5-1   Family FAU_SAS
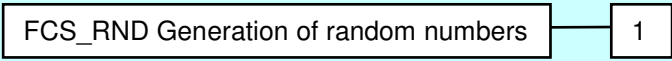
FAU_SAS Audit data storage	
Family behaviour:	This family defines functional requirements for the storage of audit data.
Component leveling:	FAU_SAS Audit data storage ——— 1
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2   Definition of the family FCS_RND

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

The family 'Generation of random numbers (FCS_RND)' is specified as follows:

Table 5-2   Family FCS_RND
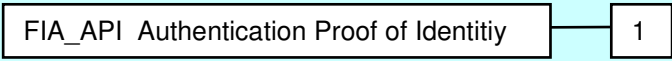
FCS_RND Generation of random numbers	
Family behaviour:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component leveling:	FCS_RND Generation of random numbers —— 1
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3   Definition of the family FIA_API

To describe the security requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [R6]. This family describes the functional requirements for the proof of a the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application Note 29: *The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the CC part 2 (cf.* [R12] *"Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.*

Table 5-3   Family FIA_API
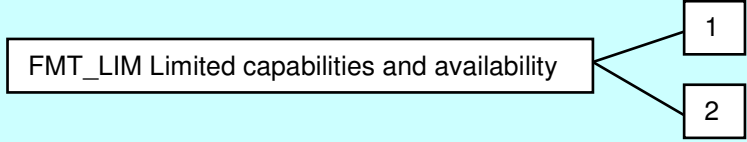
FIA_API Authentication Proof of Identity	
Family behaviour:	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
Component leveling:	FIA_API Authentication Proof of Identitiy ——— 1
FIA_API.1	Authentication Proof of Identity.
Management:	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or rule*].

5.4   Definition of the family FMT_LIM

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

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

Table 5-4   Family FMT_LIM

FMT_LIM Limited capabilities and availability	
Family behaviour:	This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
Component leveling:	FMT_LIM Limited capabilities and availability — 1 / 2
FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

FMT_LIM.2	Limited availability
Hierarchical to:	No other components
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application Note 30:   *the functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that*

> *1. the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced*

or conversely

- *the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.*
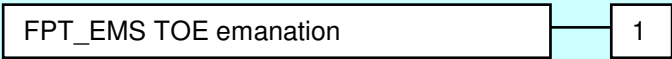
The combination of both requirements shall enforce the related policy.

5.5   Definition of the family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [R6].

The family 'TOE Emanation (FPT_EMS)' is specified as follows:

Table 5-5   Family FPT_EMS

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

6.   Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 [R10] of the CC. Each of these operations is used in this PP.

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

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

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text. Assignments that have been made by the ST author are denoted as **bold underlined text** and the original text of the component is given by a footnote. In some cases the assignment made by the PP authors defines a selection performed by the ST author. Thus this text is underlined and italicized like *this*.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [R11]. The operation "load" is synonymous to "import" used in [R11].
Table 6-1 provides the definition of security attributes.

Table 6-1   Definition of security attributes

Security attribute	Values	Meaning
Terminal authentication status	None (any Terminal)	Default role (i.e.without authorisation after start-up)

Security attribute	Values	Meaning
	CVCA	Roles defined in the certificate used for authentication (cf. [R8]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	Roles defined in the certificate used for authentication (cf. [R8]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	Roles defined in the certificate used for authentication (cf. [R8]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	Roles defined in the certificate used for authentication (cf. [R8]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [R8])
	DG3 (Fingerprint)	Read access to DG3: (cf. [R8])
	DG3(Fingerprint)/DG4 (Iris)	Read access to DG3 and DG4: (cf. [R8])

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

Table 6-2　Keys and certificates

Name	Data

Name	Data
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the travel document Issuer signs the Document Signer Public Key Certificate (C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA}) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK_{CSCA}) The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) to be distributed by strictly secure diplomatic means, see. [R18], 5.5.1.
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO_D) of the travel document with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS}).
PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [R20].
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)	The ephemeral PACE Authentication Key Pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE) is used fot Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03110 [R8], cf [R20].
Ephem-PKPICC-PACE	PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [R9], cf. [R20].
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifiying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifiying Certification Authority Certificate or of a domestic Document Verifier Certificate.

Name	Data
Country Verifying Certification Authority Certificate (C$_{CVCA}$)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [R8] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK$_{CVCA}$) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C$_{DV}$)	The Document Verifier Certificate C$_{DV}$ is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK$_{DV}$) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C$_{IS}$)	The Inspection System Certificate (C$_{IS}$) ssued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK$_{IS}$) () the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK$_{ICC}$, PK$_{ICC}$) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [11].
Chip Authentication Public Key (PK$_{ICC}$)	The Chip Authentication Public Key (PK$_{ICC}$) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK$_{ICC}$)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itselfas authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organisation signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organisation with the Document Signer Public Key.

Name	Data
Chip Authentication Session Keys	Secure Messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
Active Authentication Key Pair	The Active Authentication Key Pair (SK_{AA}, PK_{AA}) is used for the Active Authentication mechanism in accordance with [R18].
Active Authentication Public Key (PK_{AA})	The Active Authentication Public Key (PK_{AA}) is stored in the EF.DG15. These keys are used by Inspection Systems to confirm the genuinity of the travel document's chip.
Active Authentication Private Key (SK_{AA})	The Active Authentication Private Key (SK_{AA}) is used by the TOE to authenticate itself as genuine travel document's chip.

Application Note 31: *The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organisation.*

6.1   Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

6.1.1.1   FAU_SAS.1 Audit storage

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (CC part 2).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1	The TSF shall provide the Manufacturer[21] with the capability to store the IC Identification Data[22] in the audit records.

---

[21] [assignment: *authorised user*]
[22] [assignment: *list of audit information*]

Application Note 32:   *The Manufacturer role is the default user identity assumed by the TOE in the life cycle Phase 2 Manufacturing. The IC manufacturer and the travel document Manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF-Data into the TOE. The audit records are write-only-once data of the travel document's chip (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).*

6.1.2 Class Cryptographic Support (FCS)

6.1.2.1   FCS_CKM.1 Cryptographic key generation

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

FCS_CKM.1/DH_PACE Cryptographic key generation   - Diffie-Hellman for PACE session keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: not fulfilled but justified.
Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/ DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:
	1. **Diffie-Hellman (DH) key derivation Protocol compliant PKCS#3 [R38]**[23] and specified cryptographic key sizes: **1024 - 2048 bit**[24], and
	2. **Elliptic Curve Diffie-Hellman (ECDH) compliant to BSI TR-03111 v2.00 [R9]**[25] and specified cryptographic key sizes: **160 bit – 521 bit**[26],
	that meet the following: ICAO TR-SAC [R20][27].

---

[23] [selection: *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111*]

[24] [assignment: *cryptographic key sizes*]

[25] [selection: *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111*]

[26] [assignment: *cryptographic key sizes*]

[27] [assignment: *list of standards*]

Application Note 33: *The TOE generates a shared secret value K with the terminal during the PACE protocol, see [R20]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R38]) or on the ECDH compliant to TR-03111 [R9] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [R20] and [R9] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K$_{MAC}$, PACE-K$_{ENC}$) according to [R20] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.*

Application Note 34: *FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R20].*

FCS_CKM.1/CA Cryptographic key generation - Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
                              FCS_COP.1   Cryptographic   operation]:   fulfilled   by
                              FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC
                              FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: **specified in BSI TR-03110 v2.10 part 3, Annex A.2.3 [R8]**[28] and specified cryptographic key sizes 1. **For DH: 1024- 2048 bit**[29], 2. **For ECDH : 160 bit – 521 bit**[30], that meet the following: 1. **For DH: based on the Diffie-Hellman key derivation protocol compliant to PKCS#3 [R38] and BSI TR-03110 part 1 [R8]** 2. **For ECDH: based on an ECDH protocol compliant to BSI TR-03111 [R9]**

Application Note 35: *FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R8].*

Application Note 36: *The TOE generates a shared secret value with the terminal during the Chip Authentication protocol Version 1, see [R8]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R38]) or on the ECDH compliant to TR-03111 [R9] (i.e. the elliptic curve cryptographic algorithm (cf. [R9] for details). The shared secret value is used to derive the*

---

[28] [assignment: *list of standards*]
[29] [assignment: *cryptographic key sizes*]
[30] [assignment: *cryptographic key sizes*]

Chip Authentication session keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [R8]).

Application Note 37: *The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 uses SHA-1 (cf. [R8]). The TOE implement hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [R8] for details).*

6.1.2.2   FCS_CKM.4 Cryptographic key destruction – Session keys

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (CC part 2).

FCS_CKM.4 Cryptographic key destruction – Session keys

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
                                FDP_ITC.2 Import of user data with security attributes, or
                                FCS_CKM.1   Cryptographic   key   generation]:   fulfilled   by
FCS_CKM.1/DH_PACE and FCS_CKM.1/CA

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **physical deletion by overwriting the memory data with zeros**[31] that meets the following: **none**[32].

Application Note 38: *The TOE shall destroy any session keys in accordance with FCS_CKM.4 after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.*

6.1.2.3   FCS_COP.1 Cryptographic operation

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (CC part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/AA_SIGN   Cryptographic operation – Signature for Active Autentication

---

[31] [assignment: *cryptographic key destruction method*]
[32] [assignment: *list of standards*]

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
                        FDP_ITC.2 Import of user data with security attributes, or
                        FCS_CKM.1 Cryptographic key generation]
                        FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ AA_SIGN	The TSF shall perform digital signature for Active Authentication data in accordance with a specific cryptographic algorithm **RSA with SHA-256**[33] and cryptographic key sizes **1024 - 2048 bits**[34]that meet the following: **the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital Signature scheme 1 [R24]) used for Active Authentication defined by ICAO Doc 9303 Part 1 [R21] [35].**

Application Note 39: *This SFR has been added by the ST author to specify the cryptographic algorithm and key sizes used by the TOE to perform an Active Authentication in accordance with ICAO Doc 9303 part 1 [R21].*

FCS_COP.1/PACE_ENC   Cryptographic   operation   –   Encryption/Decryption AES/3DES for PACE protocol

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
                        FDP_ITC.2 Import of user data with security attributes, or
                        FCS_CKM.1   Cryptographic   key   generation]:   fulfilled   by
                        FCS_CKM.1/DH_PACE
                        FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption[36] in accordance with a specified cryptographic algorithm **AES and 3DES** in CBC mode[37] and cryptographic key sizes **112 (for 3DES),** and **128, 192 and 256 bit (for AES)**[38] that meet the following: **ICAO TR-SAC [R20]**[39].

Application Note 40: *This SFR requires the TOE to implement the cryptographic primitive AES and 3DES for secure messaging with encryption of the transmitted data and*

---

[33] [assignment: *cryptographic algorithm*]
[34] [assignment: *cryptographic key sizes*]
[35] [assignment: *list of standards*]
[36] [assignment: *list of cryptographic operations*]
[37] [selection: *AES, 3DES*]
[38] [assignment: *cryptographic key sizes*]
[39] [assignment: *list of standards*]

encryption of the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to FCS_CKM.1/DH_PACE (PACE-K$_{ENC}$)

FCS_COP.1/PACE_MAC Cryptographic operation – MAC for PACE protocol

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation] : fulfilled by
FCS_CKM.1/DH_PACE
FCS_CKM.4 Cryptographic key destruction : fulfilled by FCS_CKM.4

FCS_COP.1.1/ PACE_MAC	The TSF shall perform <u>secure messaging – message authentication code</u>[40] in accordance with a specified cryptographic algorithm **CMAC and Retail MAC**[41] and cryptographic key sizes **112, 128, 192 and 256 bit**[42] that meet the following: **ICAO TR-SAC [R20]**[43].

Application Note 41:   *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K$_{MAC}$). Note that in accordance with [4] the (two-key) Triple-DES could be used in Retail mode for secure messaging.*

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption/Decryption for CA protocol

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ CA_ENC	The TSF shall <u>perform secure messaging – encryption and decryption</u>[44] in accordance with a specified cryptographic algorithm **AES and 3DES**[45] and cryptographic key sizes **112 (for 3DES)** and **128, 192 and 256 bit (for AES)**[46] that meet the

---

[40] [assignment: *list of cryptographic operations*]
[41] [selection: CMAC, Retail-MAC]
[42] [selection: 112, 128, 192, 256]
[43] [assignment: *list of standards*]
[44] [assignment: *list of cryptographic operations*]
[45] [assignment: *cryptographic algorithm*]
[46] [assignment: *cryptographic key sizes*]
[47] [assignment: *list of standards*]

following: **BSI TR-03110 [R8]**[47].

Application Note 42: *This SFR requires the TOE to implement the cryptographic primitives (i.e. 3DES and AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA*

FCS_COP.1/CA_MAC Cryptographic operation – MAC for CA protocol

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ CA_MAC	The TSF shall perform <u>secure messaging – message authentication code</u>[48] in accordance with a specified cryptographic algorithm **CMAC and Retail MAC**[49] and cryptographic key sizes **112, 128, 192 and 256 bit**[50] that meet the following: **BSI TR-03110 [R8]**[51].

Application Note 43: *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as travel document Manufacturer or Personalisation Agent by means of the authentication mechanism.*

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

---

[48] [assignment: *list of cryptographic operations*]
[49] [selection: CMAC, Retail-MAC]
[50] [selection: 112, 128, 192, 256]
[51] [assignment: *list of standards*]

FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification[52] in accordance with a specified cryptographic algorithm 1. **RSA as specified in** 2. **Table** 6-3[53] and cryptographic key sizes: **bit length of the modulus equal to 1024, 1280, 1536, 2048 or 3072** [54] that meet the following: **RSA PKCS#1 [R37]**[55]and 3. **ECDSA with SHA-1, SHA-224 or SHA-256 as specified in Table 6-4**[56] and cryptographic key sizes: **160, 192, 224 or 256 bit**[57] that meet the following: **BSI TR-03111 [R9]**.

Table 6-3   RSA algorithms for signature verification in Terminal Authentication

Object Identifier	Signature	Hash	Parameters
id-TA-RSA-v1-5-SHA-1	RSASSA-PKCS1-v1_5	SHA-1	N/A
id-TA-RSA-v1-5-SHA-256	RSASSA-PKCS1-v1_5	SHA-256	N/A
id-TA-RSA-PSS-SHA-1	RSASSA-PSS	SHA-1	Default
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	Default

Table 6-4   ECDSA algorithms for signature verification in Terminal Authentication

Object Identifier	Signature	Hash
id-TA-ECDSA-SHA-1	ECDSA	SHA-1
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256

Application Note 44:   *The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.*

6.1.2.4   FCS_RND.1 Quality metrics for random numbers

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (CC part 2 extended).

---

[52] [assignment: *list of cryptographic operations*]
[53] [assignment: *list of cryptographic operations*]
[54] [assignment: *cryptographic key sizes*]
[55] [assignment: *list of standards*]
[56] [assignment: *list of cryptographic operations*]
[57] [assignment: *cryptographic key sizes*]

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **BSI AIS-31 functionality class P2 [R3]**[58].

Application Note 45:   *This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols as required by FIA_UAU.4.*

6.1.3 Class FIA Identification and Authentication

For the sake of better readability, Table 6-5 provides an overview of the authentication mechanisms used.

---

[58] [assignment: *a defined quality metric*]

Table 6-5   Overview on authentication SFRs

Mechanism	SFR for the TOE	Comments
Authentication Mechanism for Personalization Agents	FIA_UAU.4	3DES (112 bit keys) Retail MAC (112 bit keys)
Chip Authentication Protocol v.1	FIA_API.1/CA FIA_UAU.5, FIA_UAU.6	3DES (112 bit keys) AES (128, 192 and 256 bit keys) CMAC (128, 192 and 256 bit keys) Retail MAC (112 bit keys) DH ECDH
Terminal Authentication Protocol v.1	FIA_UAU.5	RSASSA-PKCS1-v1_5 RSASSA-PSS ECDSA
PACE protocol[59]	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE	3DES (112 bit keys) AES (128, 192 and 256 bit keys) CMAC (128, 192 and 256 bit keys) Retail MAC (112 bit keys) Integrated Mapping Generic mapping DH ECDH
Active Authentication	FIA_API.1/AA	RSA with SHA-256

Note the Chip Authentication Protocol Version 1 as defined in this security target includes:
- the asymmetric key agreement to establish symmetric secure messaging between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

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

FIA_AFL.1/PACE   Authentication failure handling – PACE authentication using non-blocking authorisation data

> Hierarchical to: No other components.

> Dependencies: FIA_UAU.1   Timing   of   authentication: fulfilled   by FIA_UAU.1/PACE

---

[59] Only listed for information purposes

FIA_AFL.1.1/PACE	The TSF shall detect when a **defined integer number between 1 and 255**[60] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall **send the response to the authentication request with a few seconds delay.**

Application Note 46: *The count of consecutive unsuccessful authentications is stored in non-volatile memory and is preserved across power-up and power-down cycles. After a successful authentication the count is reset to zero.*

6.1.3.1   FIA_UID.1 Timing of identification

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (CC part 2).

FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to [R20], 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 [R8][61] 5. to carry out the Terminal Authentication Protocol v.1 according to [R8][62] 6. **to carry out the Active Authentication Mechanism**[63] on behalf of the user to be performed before the user is identified**.**
FIA_UID.1.2/PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

---

[60] [assignment: *positive integer number*]
[61] [assignment: *list of TSF-mediated actions*]
[62] Only listed for information purposes
[63] [assignment: *list of TSF-mediated actions*]

Application Note 47:   *The SFR FIA_UID.1/PACE in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in the PACE PP [R7] by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 48:   *In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The travel document Manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 "Personalisation of the travel document". The users in role "travel document Manufacturer" or "Personalisation Agent" identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1.*

Application Note 49:   *User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).*

Application Note 50:   *In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.*
Please note that a travel document Manufacturer or a Personalisation Agent act on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

6.1.3.2   FIA_UAU.1 Timing of authentication

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

FIA_UAU.1/PACE Timing of authentication

      Hierarchical to: No other components.

      Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1/PACE	The TSF shall allow
	1. <u>to establish the communication channel,</u>
	2. <u>carrying out the PACE Protocol according to [R20]</u>,
	3. <u>to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,</u>
	4. <u>to identify themselves by selection of the authentication key,</u>
	5. <u>to carry out the Chip Authentication Protocol Version 1 according to [R8][64]</u>,
	6. <u>to carry out the Terminal Authentication Protocol Version 1 according to [R8][65]</u>,
	7. **<u>to carry out the Active Authentication mechanism</u>**[66]
	on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 51:   *The SFR FIA_UAU.1/PACE in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in the PACE PP [R7] by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 52:   *The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}), cf. FTP_ITC.1/PACE.*

6.1.3.3   FIA_UAU.4 Single-use authentication mechanisms

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (CC part 2).

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

      Hierarchical to: No other components.

      Dependencies: No dependencies.

---

[64] [assignment: *list of TSF-mediated actions*]
[65] [assignment: *list of TSF-mediated actions*]
[66] [assignment: *list of TSF-mediated actions*]

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. <u>PACE Protocol according to [R20],</u> 2. <u>Authentication Mechanism based on **AES and 3DES**[67]</u>, 3. <u>Terminal Authentication Protocol v.1 according to [R8][68].</u>

Application Note 53: *The SFR FIA_UAU.4.1 in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [R7].*

Application Note 54: *The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. In addition, the authentication of Personalisation Agent and of travel document Manufacturer make use of a diversifier, thus ensuring protection against replay attacks.*

6.1.3.4   FIA_UAU.5 Multiple authentication mechanisms

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (CC part 2).

FIA_UAU.5/PACE Multiple authentication mechanisms

 Hierarchical to: No other components.

 Dependencies: No dependencies.

FIA_UAU.5.1/PACE	The TSF shall provide 1. <u>PACE Protocol according to [R20],</u> 2. <u>Passive Authentication according to [R18],</u> 3. <u>Secure messaging in MAC-ENC mode according to [R20],</u> 4. <u>Symmetric Authentication Mechanism based on **AES and 3DES**[69]</u> 5. <u>Terminal Authentication Protocol v.1 according to [R8][70]</u> to support user authentication.

---

[67] [selecion: *Triple-DES, AES or other approved algorithms*]
[68] [assignment: *identified authentication mechanism(s)*]
[69] [selection: *Triple-DES, AES or other approved algorithms*]
[70] [assignment: *list of multiple authentication mechanism(s)*]

FIA_UAU.5.2/PACE	The TSF shall authenticate any user's claimed identity according to the <u>following rules:</u> 1. <u>Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol,</u> 2. <u>The TOE accepts the authentication attempt as Travel Document Manufacturer by</u> **the Authentication Mechanism with Travel Document Manufacturer Keys**[71]. 3. <u>The TOE accepts the authentication attempt as Personalization Agent by</u> **the Authentication Mechanism with Personalization Agent Keys**[72]. 4. <u>After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1</u> 5. <u>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</u>[73]

Application Note 55: *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 ePassport application..*

Application Note 56: *The Travel Document Manufacturer authentication uses a key diversification algorithm based on data randomly chosen by the card.*

Application Note 57: *The SFR FIA_UAU.5.1/PACE in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.*

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

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (CC part 2).

---

[71] [selection: *the Authentication Mechanism with Personalization Agent Keys*]
[72] [selection: *the Authentication Mechanism with Personalization Agent Keys*]
[73] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions <u>each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the PACE terminal</u>[74].

Application Note 58:   *The PACE protocol specified in [R20] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.*

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC	The TSF shall re-authenticate the user under the conditions <u>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</u>[75].

Application Note 59:   *The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [R18] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user*.

---

[74] [assignment: *list of conditions under which re-authentication is required*]
[75] [assignment: *list of conditions under which re-authentication is required*]

6.1.3.6   FIA_API.1 Authentication Proof of Identity

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (CC part 2 extended).

FIA_API.1/CA Authentication Proof of Identity by Chip Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA	The TSF shall provide a <u>Chip Authentication Protocol Version 1 according to [R8][76]</u> to prove the identity of the <u>TOE[77]</u>.

Application Note 60: *This SFR requires the TOE to implement the Chip Authentication Mechanism Version 1 specified in [R8]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [R18]. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication key (EF.DG14).*

FIA_API.1/AA   Authentication Proof of Identity by Active Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA	The TSF shall provide a <u>Active Authentication Protocol according to [R18][78]</u> to prove the identity of the <u>TOE[79]</u>.

6.1.4 Class FDP User Data Protection

6.1.4.1   FDP_ACC.1 Subset access control

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

FDP_ACC.1/TRM Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

---

[76] [assignment: *authentication mechanism*]
[77] [assignment: *authorized user or rule*]
[78] [assignment: *authentication mechanism*]
[79] [assignment: *authorized user or rule*]

FDP_ACC.1.1/TRM	The TSF shall enforce the <u>Access Control SFP</u>[80] on <u>terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document</u>[81].

Application Note 61: *The SFR FIA_ACC.1.1 in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.*

6.1.4.2   FDP_ACF.1 Security attribute based access control

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (CC part 2).

FDP_ACF.1/TRM Security attribute based access control – Terminal Access

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM
FMT_MSA.3 Static attribute initialization: not fulfilled, but justified

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

FDP_ACF.1.1 /TRM	The TSF shall enforce the <u>Access Control SFP</u>[82] to objects based on the following:
	   1. <u>Subjects:</u>
	     a. <u>Terminal,</u>
	     b. <u>BIS-PACE,</u>
	     c. <u>Extended Inspection System</u>
	
	   2. <u>Objects:</u>
	     a. <u>data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,</u>
	     b. <u>data in EF.DG3 of the logical travel document</u>
	     c. <u>data in EF.DG4 of the logical travel document</u>
	     d. <u>all TOE intrinsic secret cryptographic keys stored in</u>

---

[80] [assignment: *access control SFP*]
[81] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[82] [assignment: *access control SFP*]

	the travel document[83],

	3. Security attributes:
	   a. PACE Authentication
	   b. Terminal Authentication v.1,
	   c. Authorisation of the Terminal[84].
	-

FDP_ACF.1.2/TRM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [R20] after a successful PACE authentication as required by FIA_UAU.1/PACE**[85]**.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[86].
FDP_ACF.1.4 /TRM	The TSF shall explicitly deny access of subjects to objects based on the following rules: 1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document 2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document 3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM. 4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM 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[87]

---

[83] [e.g. Chip Authentication Version 1 and ephemeral keys]
[84] [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[85] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations or controlled objects*]
[86] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[87] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

Application Note 62:   *The read access to user data in the personalization phase is protected by a Restricted Application Secret Code.*

Application Note 63:   *The SFR FDP_ACF.1.1/TRM in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [R7]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.*

Application Note 64:   *The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [R8]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.*

Application Note 65:   *Please note that the Document Security Object (SO$_D$) stored in EF.SOD (see [R18]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [R20].*

Application Note 66:   *FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).*

Application Note 67:   *Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.*

6.1.4.3   FDP_RIP.1 Subset residual information protection

The TOE shall meet the requirement "Subset residual information protection" (FDP_RIP.1)" as specified below (CC part 2).

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from[88]** the following objects.
	1. Session Keys (immediately after closing related communication session),
	2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K[89])[90]

6.1.4.4 FDP_UCT.1 Basic data exchange confidentiality

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (CC part 2).

FDP_UCT.1/TRM   Basic data exchange confidentiality - MRTD

> Hierarchical to: No other components.

> Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
> FTP_TRP.1 Trusted path]: fulfilled by FPT_ITC.1/PACE
> [FDP_ACC.1 Subset access control, or
> FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM

FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP[91] to be able to transmit and receive[92] user data in a manner protected from unauthorized disclosure.

6.1.4.5 FDP_UIT.1 Basic data exchange integrity

The TOE shall meet the requirement "Basic data exchange integrity (FDP_UIT.1)" as specified below (CC part 2).

FDP_UIT.1/TRM   Data exchange integrity

> Hierarchical to: No other components.

> Dependencies: [FDP_ACC.1 Subset access control, or
> FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM
> [FTP_ITC.1 Inter-TSF trusted channel, or
> FTP_TRP.1 Trusted path]: fulfilled by FTP_ITC.1/PACE

---

[88] [selection: *allocation of the resource to, deallocation of the resource from*]
[89] According to [R20]
[90] [assignment: *list of objects*]
[91] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[92] [selection: *transmit, receive*]

| FDP_UIT.1.1/TRM | The TSF shall enforce the <u>Access Control SFP</u>[93] to be able to <u>transmit and receive</u>[94] user data in a manner protected from <u>modification, deletion, insertion and replay</u>[95] errors |
| FDP_UIT.1.2/TRM | The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u>[96] has occurred. |

6.1.5 Class FTP Trusted Path/Channels

6.1.5.1   FTP_ITC.1/PACE   Inter-TSF trusted channel after PACE

FTP_ITC.1/PACE   Inter-TSF trusted channel after PACE

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall enforce communication via the trusted channel for <u>any data exchange between the TOE and the Terminal</u>[97].

Application Note 68:   *The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.*

Application Note 69:   *The trusted channel is established after successful performing the Chip Authentication protocol or the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K$_{MAC}$, PACE-K$_{ENC}$); If the Chip Authentication protocol was successfully performed, secure messaging is immediately restarted using the derived session keys. This secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.*

---

[93] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[94] [selection: *transmit, receive*]
[95] [selection: *modification, deletion, insertion, replay*]
[96] [selection: *modification, deletion, insertion, replay*]
[97] [assignment: *list of functions for which a trusted channel is required*]

Application Note 70: *Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.*

6.1.6 Class FMT Security Management

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

6.1.6.1   FMT_SMF.1 Specification of Management Functions

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

FMT_SMF.1 Specification of Management Functions

>   Hierarchical to: No other components.

>   Dependencies: No Dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-Personalization, 3. Personalization, 4. Configuration[98].

Application Note 71: *The ability to initialize, personalize and configure the TOE is restricted to a successfully authenticated travel document Manufacturer or Personalization Agent by means of symmetric keys. Travel document Manufacturer Keys are only active in uninitialized products. Personalization Agent Keys are only active in initialized but not personalized products. The MRTD locks out after a programmable number of consecutive unsuccessful authentication attempts. The Travel document Manufacturer Keys are disabled once initialization is complete*

6.1.6.2   FMT_SMR.1 Security roles

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (CC part 2).

FMT_SMR.1/PACE   Security roles

---

[98] [assignment: *list of security management functions to be provided by the TSF*]

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	The TSF shall maintain the roles:
	1. Manufacturer,
	2. Personalization Agent,
	3. Terminal,
	4. PACE authenticated BIS-PACE,
	5. Country Verifying Certification Authority,
	6. Document Verifier,
	7. Basic Inspection System
	8. Domestic Extended Inspection System,
	9. Foreign Extended Inspection System[99].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application Note 72: *The SFR FMT_SMR.1.1/PACE in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.*

Application Note 73: *For explanation on the role Manufacturer and Personalisation Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the travel document presenter).*

The TOE recognises the travel document holder or an authorised other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (FIA_UAU.1/PACE).

Application Note 74: *SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.*

6.1.6.3   FMT_LIM.1 Limited capabilities

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (CC part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

---

[99] [assignment: *the authorised identified roles*]

FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow: 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[100].

6.1.6.4   FMT_LIM.2 Limited availability

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (CC part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1	The TSF shall be designed in a manner that limits their 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 disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. sensitive User Data (EF.DG3 and EF.DG4) to e disclosed,[101].

Application Note 75:   *The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*
Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.1.6.5   FMT_MTD.1 Management of TSF data

---

[100] [assignment: *limited capability and availability policy*]
[101] [assignment: *limited capability and availability policy*]

Application Note 76: *the following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.*

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (CC part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions; fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[102] the Initialization Data and Pre-personalization Data[103] to the Manufacturer[104].

Application Note 77: *Initialization Data are written by the IC Manufacturer and Pre-personalization Data are written by the Travel document Manufacturer, according to the description given in section 1.5.3. The Initialization Data include the travel document Manufacturer Keys.*

FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to read out[105] the Initialization Data and the Pre-personalisation Data[106] **to the Personalisation Agent**[107].

Application Note 78: *The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write*

---

[102] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[103] [assignment: *list of TSF data*]
[104] [assignment: *the authorised identified roles*]
[105] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[106] [assignment: *list of TSF data*]
[107] [assignment: *the authorised identified roles*]

the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to <u>write</u>[108] the: 1. <u>initial Country Verifying Certification Authority Public Key,</u> 2. <u>initial Country Verifying Certification Authority Certificate,</u> 3. <u>initial Current Date</u>[109] to **the Personalization Agent**[110].

Application Note 79:   *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [R8]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.*

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to <u>update</u>[111] the: 1. <u>Country Verifying Certification Authority Public Key,</u> 2. <u>Country Verifying Certification Authority</u>

---

[108] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[109] [assignment: *list of TSFdata*]
[110] [assignment: *the authorised identified roles*]

	Certificate[112],
	to Country Verifying Certification Authority[113].

Application Note 80: *The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [R8]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [R8]).*

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

> Hierarchical to: No other components.

> Dependencies: FMT_SMF.1 Specification of management functions
> FMT_SMR.1 Security roles

FMT_MTD.1.1/DATE	The TSF shall restrict the ability to modify[114] the Current Date[115] to: 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System[116]

Application Note 81: *The authorized roles are identified in their certificate (cf. [R8]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [R8]).*

FMT_MTD.1/ADDTSF_WRITE Management of TSF data – Additional TSF data Write

> Hierarchical to: No other components.

> Dependencies: FMT_SMF.1 Specification of management functions
> FMT_SMR.1 Security roles

FMT_MTD.1.1/ ADDTSF_WRITE	The TSF shall restrict the ability to write[117] **the Security Environment object** to the Personalization Agent[118].

---

[111] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*
[112] [assignment: *list of TSF data*]
[113] [assignment: *the authorised identified roles*]
[114] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]]*
[115] [assignment: *list of TSF data*]
[116] [assignment: *the authorised identified roles*]
[117] [selection: *change_default, query, modify, dolete, clear, [assignment: other operations]]*
[118] [assignment: *the authorised identified roles*]

Application Note 82:   *This SFR has been added by the ST author to impose a restriction in writing the internal data object called "Security Environment Object". This object stores links to the PACE keys, the Active Authentication private key, the Chip Authentication private key and the trustpoint.*

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

      Hierarchical to: No other components.

      Dependencies: FMT_SMF.1 Specification of management functions
                              FMT_SMR.1 Security roles

FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to **load**[119] the Chip Authentication Private Key[120] to **the Travel document Manufacturer**[121]

Application Note 83:   *The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.*

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

      Hierarchical to: No other components.

      Dependencies: FMT_SMF.1 Specification of management functions
                              FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read[122]: 1. PACE passwords, 2. Chip Authentication Private key, 3. Personalization Agent Keys. 4. **Active Authentication Private Key**[123] to none[124].

Application Note 84:   *The SFR FMT_MTD.1/KEY_READ in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.*

---

[119] [selection: *create, load*]
[120] [assignment: *list of TSF data*]
[121] [assigned: *the authorised identified roles*]
[122] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[123] [assignment: *list of TSF data*]
[124] [assignment: *the authorised identified roles*]

Application Note 85: *A refinement has been added to address the Active Authentication mechanism..*

FMT_MTD.1/PA   Management of TSF data – Personalisation Agent

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ PA	The TSF shall restrict the ability to write[125] the Document Security Object (SO$_D$)[126] to the Personalisation Agent[127].

Application Note 86: *By writing SO$_D$ into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness of all the personalisation data related. This consists of user- and TSF-data .*

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to write[128] the **Active Authentication Private Key**[129] to **the Travel Document Manufacturer**[130].

Application Note 87: *The addition of this SFR does not impair the conformance to the Protection Profiles*

6.1.6.6   FMT_MTD.3 Secure TSF data

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (CC part 2).

---

[125] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[126] [assignment: *list of TSF data*]
[127] [assignment: *the authorised identified roles*]
[128] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[129] [assignment: *list of TSF data*]
[130] [assignment: *the authorised identified roles*]

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for <u>TSF data of the Terminal Authentication Protocol v.1 and the Access Control</u>[131].

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 and the expiration date of Document Verifier Certificate is not before the Current date of the TOE,**

3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.**

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

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

Application Note 88: *The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.*

6.1.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF-data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFRs "Limited capabilities (FMT_LIM.1)",

---

[131] [assignment: l*ist of TSF data*]

"Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" together with the SAR "Security architecture description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE security functionality.

6.1.7.1   FPT_EMS.1   TOE emanation

The TOE shall meet the requirement "TOE emanation (FPT_EMS.1)" as specified below (CC part 2 extended):

FPT_EMS.1   **TOE Emanation**

> Hierarchical to: No other components.

> Dependencies: No dependencies.

FPT_EMS.1.1	The TOE shall not emit **electromagnetic and current emissions**[132] in excess of **intelligible threshold**[133] enabling access to 1. Chip Authentication session Keys, 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. Personalization Agent Keys, 5. Chip Authentication Private Key, 6. Active Authentication Private Key[134] and 7. **EF.DG1 to EF.DG16**, **EF.SOD**, **EF.COM**[135]
FPT_EMS.1.2	The TSF shall ensure any users[136] are unable to use the following interface smart card circuits contacts[137] to gain access to 8. Chip Authentication session Keys, 9. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}), 10. the ephemeral private key ephem-SK_{PICC}-PACE, 11. Personalization Agent Keys, 12. Chip Authentication Private Key, 13. Active Authentication Private Key[138] and 14. **EF.DG1 to EF.DG16**, **EF.SOD**, **EF.COM**[139]

Application Note 89:   *The SFR FPT_EMS.1.1 in this ST covers the definition in the EAC PP [R6] that, in turn, extends the definition in PACE PP [R7] by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in this ST covers the definition in the EAC PP [R6] that, in turn,*

---

[132] [assignment: *type of emissions*]
[133] [assignment: *specified limits*]
[134] [assignment: *list of types of TSF data*]
[135] [assignment: *list of types of user data*]
[136] [assignment: *type of users*]
[137] [assignment: *type of connection*]
[138] [assignment: *list of types of TSF data*]
[139] [assignment: *list of types of user data*]

extends the definition in PACE PP [7] by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

Application Note 90: *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [R23] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.*

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

6.1.7.2 FPT_FLS Failure with preservation of secure state

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria part 2).

FPT_FLS.1 **Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1[140]

6.1.7.3 FPT_TST.1 TSF testing

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

---

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

FPT_TST.1.1	The TSF shall run a suite of self tests **during initial start-up, and before any use of TSF data**[141] to demonstrate the correct operation of the TSF[142].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[143].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[144].

6.1.7.4   FPT_PHP.3 Resistance to physical attack

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (CC part 2).

FPT_PHP.3   Resistance to physical attack

> Hierarchical to: No other components.

> Dependencies: No dependencies.

| FPT_PHP.3.1 | The TSF shall resist physical manipulation and physical probing[145] to the TSF[146] by responding automatically such that the SFRs are always enforced. |

Application Note 91:   *The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.*

6.2   Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOEand its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

---

[141] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which sel test should occur]*]
[142] [selection: *[assignment: parts of TSF], the TSF*]
[143] [selection: *[assignment: parts of TSF], TSF data*]
[144] [selection: *[assignment: parts of TSF], TSF*]
[145] [assignment: *physical tampering scenarios*]
[146] [assignment: *list of TSF devices/elements*]

Table 6-6 summarizes the assurance components that define the security assurance requirements for the TOE.

Table 6-6   Assurance requirements at EAL4+

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ADV_COMP.1
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.5

Application Note 92:   *The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (OE.Prot_Logical_Travel_Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).*

6.3   Security Requirements Rationale

6.3.1 Security functional requirements rationale

Table 6-7 provides an overview for security functional requirements coverage of security objectives.

Table 6-7   Coverage of Security Objective for the TOE by SFR

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				X				X					
FCS_CKM.1/DH_PACE					X	X	X						
FCS_CKM.1/CA	X	X		X	X	X	X						
FCS_CKM.4	X			X	X	X	X						
FCS_COP.1/AA_SIGN			X				X						
FCS_COP.1/PACE_ENC							X						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FCS_COP.1/CA_ENC	X	X		X	X		X						
FCS_COP.1/PACE_MAC					X	X							
FCS_COP.1/CA_MAC	X	X		X	X								
FCS_COP.1/SIG_VER	X												
FCS_RND.1	X			X	X	X	X						
FIA_AFL.1/PACE											X		
FIA_UID.1/PACE	X			X	X	X	X						
FIA_UAU.1/PACE	X			X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X						
FIA_UAU.5/PACE	X			X	X	X	X						
FIA_UAU.6/PACE					X	X	X						
FIA_UAU.6/EAC	X				X	X	X						
FIA_API.1/CA		X											
FIA_API.1/AA			X										
FDP_ACC.1/TRM	X			X	X		X						
FDP_ACF.1/TRM	X			X	X		X						
FDP_RIP.1					X	X	X						
FDP_UCT.1/TRM	X				X		X						
FDP_UIT.1/TRM					X		X						
FMT_SMF.1		X		X	X	X	X	X					
FMT_SMR.1/PACE		X		X	X	X	X	X					
FMT_LIM.1									X				
FMT_LIM.2									X				
FMT_MTD.1/INI_ENA				X					X				
FMT_MTD.1/INI_DIS				X					X				
FMT_MTD.1/CVCA_INI	X												
FMT_MTD.1/CVCA_UPD	X												
FMT_MTD.1/DATE	X												
FMT_MTD.1/ADDTSF_WRITE	X			X									
FMT_MTD.1/CAPK	X	X			X								
FMT_MTD.1/PA				X	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X	X	X	X	X						
FMT_MTD.1/AAPK	X		X										
FMT_MTD.3	X												
FPT_EMS.1				X						X			
FPT_TST.1										X			X
FPT_FLS.1										X			X
FPT_PHP.3					X					X		X	
FDP_ITC.1/PACE					X	X	X				X		

The security objective **OT.Identification** "Identification of the TOE" addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document" addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use. The Personalization Agent also handles the security environment object according to the SFR FMT_MTD.1/ADDTSF_WRITE.

The security objective **OT.Data_Integrity** "Integrity of personal data" requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive

Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret andfor the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

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

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.

This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{ENC}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO$_D$ containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy.

The SFR FCS_RND.1 represents the general support for cryptographic operations needed.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

The Personalization Agent manages the security environment object data required for Chip Authentication and for Terminal Authentication according to SFR FMT_MTD.1/ADDTSF_WRITE.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CA proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [R8] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).
The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Active Authentication Mechanism [R18] provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Protocol defined by FIA_API.1/AA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AAPK. This key is written to the TOE as defined by FMT_MTD.1/AAPK. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/AA_SIG (for the digital signature of Active Authentication data).

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

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure
  • by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
  • by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
  • by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:
  i.   while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
  ii. for listening to PACE communication (is of importance for the current PP, since SO_D is card-individual) – FTP_ITC.1/PACE.

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

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

6.3.2 Dependency Rationale

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

Table 6-8 shows the dependencies between the SFR of the TOE.

Table 6-8   Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/AA_SIGN	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes]	Fulfilled by FCS_ITC.1/PACE
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4 from [7]
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with	Fulfilled by FCS_CKM.1/CA,

SFR	Dependencies	Support of the Dependencies
	security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [7]
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identfication	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM, justification 1 for non-satisfied dependencies
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1 from [7]

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ADDTSF_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/ PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.

Justifications for non-satisfied dependencies between the SFR for TOE:

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

6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an

attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.2 has the following dependencies:
- ADV_ARC.1 Security architecture description
- ADV_TDS.3 Basic modular design
- ADV_FUN.1 Functional testing

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

The component AVA_VAN.5 depends on:
- ADV_ARC.1, Security architectural description
- ADV_FSP.4, Security enforcing functional specification
- ADV_TDS.3, Basic modular design
- ADV_IMP.1, Implementation representation of the TSF
- AGD_OPE.1, Operational user guidance
- AGD_PRE.1, Preparative procedures
- ATE_DPT.1, Testing: basic design

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

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

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

The dependency analysis in section 6.3.2 Dependency Rationale shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.
All subjects and objects addressed by more than one SFR in section 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these "shared" items.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional assurance dependencies which are not met, a possibility which has been shown not to arise in section 6.3.2 "Dependency Rationale" and 6.3.3 Security Assurance

Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7.   TOE Summary Specification

The following sections provide a general understanding of how the TOE is implemented. To facilitate reading, the description of the security features of the TOE is organized in security services. A requirements traceability matrix against each security service is given in Table 7-2.

7.1   Coverage of SFRs

7.1.1 SS.AUTH_IDENT   Identification & Authentication

This security service meets the following SFRs:
FIA_UID.1/PACE,   FIA_UAU.1/PACE,   FIA_UAU.4/PACE,   FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_AFL.1/PACE, FCS_CKM.4, FIA_API.1/CA, FIA_API/AA, FCS_COP.1/AA_SIG, FDP_RIP.1

Access to functions and data of the TOE is only allowed to authenticated users. The authentication mechanism applied depends on the inspection system. Table 7-1 summarizes the authentication mechanisms for the various systems.

Table 7-1   Summary of authentication mechanisms

System type	MRTD Life-Cycle status	Authentication Mechanism
Pre-personalization system	Non-Initialized	Symmetric authentication based on 3DES with the 112-bit Travel document Manufacturer Keys
Personalization System	Initialized	Symmetric authentication based on 3DES with the 112-bit Personalization Agent Keys
Basic Inspection System – without PACE (BIS)	Operational	BAC based on 3DES with 112-bit Document Basic Access Keys.
Basic Inspection System supporting PACE (BIS-PACE)	Operational	PACE with either DH or ECDH key agreement. Both Generic mapping and Integrated Mapping are supported.
Extended Inspection System not supporting PACE	Operational	BAC with 3DES algorithm with Document Basic Access Keys. Chip Authentication with either DH or ECDH key agreement Terminal Authentication with either RSA or ECDSA signature verification algorithms. Active Authentication with RSA and SHA-256.
Extended Inspection System supporting PACE	Operational	PACE protocol with either DH or ECDH key agreement. Both Generic mapping and Integrated Mapping are supported. Chip Authentication with either DH or ECDH key agreement Terminal Authentication with either RSA or ECDSA signature verification algorithms. Active Authentication with RSA and SHA-256.

The travel document Manufacturer and the Personalization Agent authenticates themselves to the e-Passport by means of a mutual authentication mechanism based on the protocol defined in EMV CPS specification, section 4.1, 5.2. [R13]. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5) and the message authentication code computation accords to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/PACE_MAC).

This function detects each unsuccessful authentication attempt. The Travel document Manufacturer and the Personalization Agent have only a limited number of authentication attempts after which the related keys are blocked.

In case of regular termination of the protocol, both parties possess authentic keying materials only known to them. The user may establish a secure messaging session (FCS_CKM.1/CPS_MRTD in [R14]) and at the end of the session, the session keys are securely erased (FCS_CKM.4).

The Basic Access System and the travel document mutually authenticate by means of a Basic Access Control mechanism based on a three pass challenge-response protocol (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE). The challenge is the random number sent from one party to the other. This random number will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and normative appendix 5 of the ICAO Doc 9303 [R18]) (FCS_COP.1/PACE_ENC), while the message authentication code is computed according to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/PACE_MAC). These authentication keys are derived by the SHA-1 algorithm (FIPS 180-2) as described in the ICAO Doc 9303, normative appendix 5 [R18] [R19].

After a successful BAC authentication, the Basic Access System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

The PACE-enabled Basic Access System and the travel document mutually authenticate by means of a   PACE V2 protocol (FIA_UID.1/PACE,   FIA_UAU.1/PACE, FIA_UAU.5/PACE).

The travel document and the Inspection System perform a Diffie-Hellman (DH or ECDH) key agreement by means of keys derived from MRZ or CAN. After a successful authentication, the generated session keys are independent of MRZ or CAN entropy. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for secure messaging encryption/decryption may be either a 3DES or AES (FCS_COP.1/PACE_ENC), the MAC algorithm may be a Retail MAC, coupled with 3DES encryption, or CMAC, coupled with AES encryption (FCS_COP.1/PACE_MAC).

After a successful PACE V2 authentication, the Inspection System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

If passport inspection is performed on an a Basic Inspection System, the travel document's authenticity may be proved executing the Active Authentication protocol. To this end, the TOE signs authenticationi data with the RSA algorithm with SHA-256 hashing (FCS_COP.1/AA_SIG, FIA_API.1/AA).

If passport inspection is performed on a General Inspection System or an Extended Inspection System, then the travel document's authenticity is proved executing the Chip Authentication Protocol. To this end two algorithms may be used: (i) a Diffie-Hellman key agreement compliant to PKCS #3 with key size up to 2048 bit or (ii) ECDH key agreement

compliant to ISO15946 with key size up to 521 bit. Chip Authentication proves that the chip is genuine and also provides strong keys for Secure Messaging (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5, FIA_API.1/CA, FCS_CKM.1/CA).

If passport inspection is performed on an Extended Inspection System, then after a successful Chip Authentication the travel document's chip recognizes that the Inspection System is entitled to access sensitive data, such as fingerprints, iris image and other data not easily available from other sources by means of the Terminal Authentication protocol (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FCS_COP.1/SIG_VER). Terminal Authentication attempts are only accepted after a successful Chip Authentication and a consequent restart of the Secure Messaging session with the strong keys computed in the Chip Authentication.
The combination of Chip Authentication and Terminal Authentication provides an implementation of the Extended Access Control mechanism.

7.1.2 SS.SEC_MSG   Secure data exchange

This security service meets the following SFRs:
FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_COP.1/PACE_ENC,
FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4,
FIA_UAU.6/PACE. FIA_UAU.6/EAC, FDP_RIP.1

This security service concerns the creation and the management of a secure communication channel for the sensitive data exchange between the TOE and the Inspection System. On this channel the data will be encrypted and authenticated with session keys (3DES and AES encryption and MAC computation) such that the TOE is able to verify the integrity and authenticity of received data. The algorithm used for encryption/decryption may either be:
- 3DES [R35] in CBC mode with key size 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5), with message authentication code computed according to Retail MAC algorithm and cryptographic key size 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).
- AES [R36] in CBC mode with key sizes 128, 192 and 256 bits, with message authentication code computed according to [R34] with MAC length of 8 bytes.

The session keys are calculated during the authentication phase (FCS_CKM.1/DH_PACE, FCS_CKM.1/CA). If a PACE or Chip Authentication protocol is executed, then the Secure Messaging is restarted using the session keys computed during that authentication. The channel will be closed in case of a received message with:
- inconsistent or missing MAC,
- wrong sequence counter,
- plain access.

After a PACE or Chip Authentication protocol has been completed, the TOE rejects those commands that cause a failure of Secure Messaging (FIA_UAU.6/PACE).
Session keys are overwritten with zeroes after usage (FCS_CKM.4).

7.1.3 SS.ACC_CNTRL   Storage and Access Control of Data Objects

This security service meets the following SFRs:
FDP_ACC.1/TRM, FDP_ACF.1/TRM, FAU_SAS.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FMT_SMF.1, FMT_SMR.1/PACE, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA,

FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/ADDTSF_WRITE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FTP_ITC.1/PACE, FMT_MTD.1/PA, FMT_MTD.1/AAPK, FDP_RIP.1

As required in FDP_ACF.1/TRM, read and write access to stored data must be controlled in different phases of the production and during operational use.

This security service ensures that the assets (user data and TSF data) can only be accessed as defined by the access right written during the personalization process and allows the access to the TOE identification data in the Personalization phase. Furthermore, the access conditions allow to differentiate the roles based on the knowledge of secret keys. Any access not explicitly allowed is denied.

The TOE identification data, the DF LDS and the Travel Document Manufacturer keys are written during the IC manufacturing by the IC Manufacturer.

The Chip Authentication key pair (public key in DG14), the Active Authentication key pair (public key in DG15), the symmetric keys for the authentication of the Personalization Agent, the passport number, the application serial number, the Application Restricted Secret Code, the EF.CardAccess and the Security Environment object are written during the initialization phase by the Travel Document Manufacturer.

The Document Basic Access Keys, the current date, the CVCA public key, the trustpoint, the EF.CVCA, the Document Number, the SAC key and the Security Environment object will be written during the personalization phase by the Personalization Agent.

After keys have been written any type of direct access to any key is not allowed.

In the operational phase access to initializrion and pre-personalization data is denied.

7.1.4 SS.LFC_MNG   Life cycle management

This security service meets the following SFRs:
FMT_SMF.1, FMT_SMR.1/PACE

It ensures that the TOE life cycle status is set in an irreversible way to mark the following phases in the given order: manufacturing, personalization and operational use. The only roles allowed to set the life cycle status are the Manufacturer and the Personalization Agent.

7.1.5 SS.SW_INT_CHECK   Software integrity check of TOE's assets

This security service meets the following SFRs:
FMT_LIM.1, FMT_LIM.2, FPT_TST.1

The TOE doesn't allow to analyze, debug or modify TOE's software during the operational use. In phase 3 and 4 no commands are allowed to load executable code. Self tests are executed at initial start-up on ROM area (this functionality is implemented by the underlying hardware).

This security service also checks the integrity of the following assets:
- application files,
- security data objects.

Integrity checks will be executed before any use of TSF data.
This SF warns the entity connected upon detection of an integrity error of the sensitive data stored within the TOE Scope of Control and preserves a secure state when failure is detected by TSF.

7.1.6 SS.SF_HW   Security features provided by the hardware

This security service meets the following SFRs: FCS_RND.1, FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.3.

The TOE benefits of a set of features provided by the integrated circuit to enforce security. The security features of the hardware platform are reported in [R40]. These security functions have already been evaluated and certified being the chip already certified; a more detailed formulation of the security functions provided by the chip can be found in the security target of the IC [R39].

7.1.7 SS.SIG_VER   Verification of digital signatures

This security service meets the following SFRs:

Terminal Autentication
FCS_COP.1/SIG_VER,   FMT_SMR.1/PACE,   FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.3

The signatures to be verified are based on (i) RSA according to PKCS#1 [R37] with key sizes up to 3072 bit or (ii) ECDSA with key sizes up to 256 (FCS_COP.1/SIG_VER).
The signature verification is performed through the check of the certificate chain up to a trusted start point (a public key of the Country Verifying Certificate Authority, see FMT_MTD.3) and the current date handling (cf. [BSI, 2.2.4]). Once a signature is recognized as valid then security roles can be maintained according to FMT_SMR.1 and the CVCA certificate and the current date can be updated (FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE).
The validity of the certificate chain is proven at the TOE current date if and only if:
  i.   the digital signature of the Inspection System Certificate, checked using the public key of the Document Verifier Certificate, is recognized as valid and the Inspection System Certificate is not expired
  ii.   the digital signature of the Document Verifier Certificate, checked using the public key in the Certificate of the Country Verifying Certification Authority, is recognized as valid and the Document Verifier Certificate is not expired
  iii.   the digital signature of the Certificate of the Country Verifying Certification Authority , checked using its own public key, is recognized as valid and certificate of the Country Verifying Certification Authority is not expired

Active Authentication
FCS_COP.1/AA_SIGN
The Inspection system can hav e aprrof of the TOE identity by verifying signatures based on the algorithm RSA with SHA-256 and cryptographic key sizes 1024 and 2048 bits that meet the following the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital Signature scheme 1 [R24].

Table 7-2 shows the coverage of SFR by the security services described above.

Table 7-2   Coverage of SFRs by security services

	SS.AUTH_IDENT Agents Identification & Authentication	SS.SEC_MSG Data exchange with Secure Messaging	SS.ACC_CNTRL Access Control of Stored Data Object	SS.LFC_MNG Life Cycle Management	SS.SW_INT_CHECK SW Integrity check of TOE's Assets	SS.SF_HW Security features provided by the hardware	SS.SIG_VER Verification of digital signatures
FAU_SAS.1			X				
FCS_CKM.1/DH_PACE		X					
FCS_CKM.1/CA		X					
FCS_CKM.4	X	X					
FCS_COP.1/PACE_ENC		X					
FCS_COP.1/PACE_MAC		X					
FCS_COP.1/CA_ENC		X					
FCS_COP.1/CA_MAC		X					
FCS_COP.1/SIG_VER							X
FCS_COP.1/AA_SIG	X						X
FCS_RND.1						X	
FIA_AFL.1/PACE	X						
FIA_UID.1/PACE	X						
FIA_UAU.1/PACE	X						
FIA_UAU.4/PACE	X						
FIA_UAU.5/PACE	X						
FIA_UAU.6/EAC	X	X					
FIA_UAU.6/PACE	X	X					
FIA_API.1/CA	X						
FIA_API.1/AA	X						
FDP_ACC.1/TRM			X				
FDP_ACF.1/TRM			X				
FDP_UCT.1/TRM			X				
FDP_UIT.1/TRM			X				
FDP_RIP.1	X	X	X				
FTP_ITC.1/PACE		X					
FMT_SMF.1			X	X			
FMT_SMR.1/PACE			X	X			X
FMT_LIM.1			X		X	X	
FMT_LIM.2			X		X	X	
FMT_MTD.1/INI_ENA			X				
FMT_MTD.1/INI_DIS			X				
FMT_MTD.1/CVCA_INI			X				X
FMT_MTD.1/CVCA_UPD			X				X
FMT_MTD.1/DATE			X				X
FMT_MTD.1/ADDTSF_WRITE			X				
FMT_MTD.1/CAPK			X				
FMT_MTD.1/KEY_READ			X				
FMT_MTD.1/PA			X				
FMT_MTD.1/AAPK			X				

FMT_MTD.3								X
FPT_EMS.1							X	
FPT_FLS.1							X	
FPT_TST.1						X	X	
FPT_PHP.3							X	

7.2 Assurance Measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [R12].

The implementation is based on a description of the security architecture of the TOE and on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. These documents, together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

The configuration management plan addresses the ALC_CMC and ALC_CMS families and enforces good practices to securely manage configuration items including, but not limiting to, design documentation, user documentation, source code, test documentation and test data.

The configuration management process guarantees the separation of the development configuration libraries from the configuration library containing the releases and also supports the generation of the TOE.

All the configuration items are managed with the help of automated tools. In particular configuration items regarding security flaws are managed with the support of an issue tracking system, while all the other configuration items are managed with the help of a version control system.

The software test process, addressing the class ATE, is machine-assisted to guarantee a repeatable error-free execution of the same test chains in both the system test and in the validation phases.

A secure delivery of the TOE is guaranteed by the application of dedicated procedures. The prevention measures, the checks and all the actions to be performed at the developer's site are described in the secure delivery procedure addressing the family ALC_DEL, while the security measures related to delivery to be applied at the user's site are defined in the pre-personalization guidance. The latter document also addresses the family AGD_PRE.

The necessary information for the passport personalization is provided by a dedicated guidance and the information for its usage after delivery to the legitimate holder is provided by the guidance for the operational use. These documents address the AGD_OPE assurance family.

To protect the confidentiality and integrity of the TOE design and implementation, the development and production environment and tools conform to the security policies defined in the documentation dedicated to the development security, which addresses the family ALC_DVS.

The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in a dedicated document addressing the assurance family ALC_LCD.

Tools and techniques adopted in the development process are documented, thus addressing the assurance family ALC_TAT.

An independent vulnerability analysis, meeting requirements of the family AVA_VAN, is conducted by a third party.

Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the platform (IC) are covered by documents from the IC manufacturer. The security recommendations described in such documents have been taken into consideration.

Table 7-3 shows the documentation that provides the necessary information related to the assurance requirements defined in this security target.

Table 7-3   Assurance Requirements documentation

Security Assurance Requirements	Documents
`ADV_ARC.1`	Description of the Security Architecture of the SOMA-c003 embedded software
`ADV_FSP.4`	Functional Specification for the SOMA-c003 embedded software
`ADV_IMP.1`	Source code of the SOMA-c003 embedded software
`ADV_TDS.3`	Description of the Design of the SOMA-c003 embedded software
`ADV_COMP.1`	Rationale for Embedded Software Design Compliance concerning the composite evaluation of the SOMA-c003 electronic passport.
`AGD_OPE.1`	Personalization Guidance for the SOMA-c003 electronic passport User Guidance for the SOMA-c003 electronic passport
`AGD_PRE.1`	Pre-personalization guidance for the SOMA-c003 electronic passport.
`ALC_CMC.4, ALC_CMS.4`	Configuration Management Plan, configuration list evidences of configuration management
`ALC_DEL.1`	Secure Delivery procedure Delivery documentation
`ALC_DVS.2`	Development security description Development security documentation
`ALC_LCD.1`	Life-cycle definition
`ALC_TAT.1`	Tools and techniques definition
`ATE_COV.2`	Coverage of Test Analysis for the SOMA-c003 Electronic Passport
`ATE_DPT.2`	Depth of Test Analysis for the SOMA-c003 Electronic Passport
`ATE_FUN.1`	Functional Test Specification for the SOMA-c003 Electronic Passport Evidences of tests
`ATE_IND.2`	Documentation related to an independent test.
`AVA_VAN.5`	Documentation related to an independent vulnerability analysis.

Assurance measures described in this section cover the assurance requirements in section 6.3.3.

8.   References

8.1   Acronyms

BAC	Basic Access Control
BIS	Basic Inspection System
C$_{DS}$	DS Public Key Certificate
CBC	Cipher-block Chaining (block cipher mode of operation)
CC	Common Criteria
COM	Common data group of the LDS (ICAO Doc 9303)
CPS	Common Personalization Standard
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO Doc 9303)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
ESW	Embedded Software
GIS	General Inspection System
IC	Integrated Circuit
IS	Inspection System
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SO$_D$	Document Security Object
SOF	Strength of Function

SPA	Simple Power Analysis
ST	Security Target
3DES	Triple DES
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TR	Technical Report
VIZ	Visual Inspection Zone

8.2   Glossary

Active Authentication	Security mechanism defined in ICAO Doc 9303 [R18] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known state or organization.
application note	Additional information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the Issuing State or Organization.
Basic Access Control	Security mechanism defined by ICAO [R18] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with the Document BAC Keys.
Basic Inspection System	An inspection system which implements the terminals part of the BAC Mechanism and authenticates themselves to the MRTD's chip using the Document BAC Keys derived from the printed MRZ data for reading the logical MRTD.
biographical data	The personalized details of the bearer of the document appearing as text in the Visual Inspection Zone (VIZ) and Machine Readble Zone (MRZ) on the biographical data page of a passport book or on a travel card or visa *[R18]*.
biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.

Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level . The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Chip Authentication	Authentication protocol used to verify the genuinity of the MRTD chip.
counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means *[R18]*.
Country Signing Certification Authority (CSCA)	Certification Authority of the Issuing State or Organization which attests the validity of certificates and digital signatures issued by the Document Signer.
Country Signing Certification Authority Certificate (C$_{CSCA}$)	Certificate of the Country Signing Certification Authority Public Key (PK$_{CSCA}$) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority (CVCA)	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.
Current Date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new keys is before the certificate expiration date of the certificate for the old key.
Document Basic Access Keys	Pair of symmetric 3DES keys used for secure messaging with encryption and message authentication of data transmitted between the MRTD's chip and the inspection system [R18]. It is derived from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.

Document Security Object	A RFC3369 CMS Signed Data Structure, signed by the Document Signer. It carries the hash values of the LDS DG's and is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}) [R18].
Document Signer	Entity delegated by the Issuing State or Organization to digitally sign the DG's present in the LDS.
eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [R18].
Extended Access Control	Security mechanism identified in BSI TR-03110 [R8] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Keys and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A role of a terminal as part of an inspection system which is in addition to the BIS authorized by the Issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait *[R18]*.
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global

	interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs.
impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document *[R18]*.
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are, for instance, used for traceability and for IC identification as MRTD's material (IC identification data).
inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity.
Inspection System	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated Circuit	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the Issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the passport) [R18].
Issuing State	The Country issuing the MRTD [R18]
Logical Data Structure	The collection of groupings of DG's stored in the optional capacity expansion technology [R18]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD	Data of the MRTD holder stored according to the LDS [R18] as specified by ICAO on the contactless IC. It presents contactless readable data including (but not limited to): 　i.　personal data of the MRTD holder 　ii.　the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 　iii.　the digitized portraits (EF.DG2), 　iv.　the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 　v.　the other data according to LDS (EF.DG5 to EF.DG16).
Machine Readable Travel Document	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read [R18].
Machine Readable Zone	Fixed dimensional area located on the front of the MRTD Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods [R18].
machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine.
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: 　i.　the file structure implementing the LDS [R18], 　ii.　the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 and EF.DG 16) and 　iii.　the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as a key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing

	State or Organization personalized the MRTD.
MRTD's chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the LDS [R18].
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Passive Authentication	Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by: i. the verification of the digital signature of the SO_D and ii. comparing the hash values of the read LDS data fields with the hash values contained in the SO_D.
Personalization	The process by which the portrait, signature and biographical data are applied to the document *[R18]*.
Personalization Agent	The agent delegated by the Issuing State or Organization to personalize the MRTD for the holder by i. establishing the identity the holder for the biographic data in the MRTD, ii. enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or the encoded iris image(s) and iii. writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Physical travel document	Travel document in the form of paper, plastic and chip using secure printing to present data including (but not limited to): i. biographical data, ii. data of the MRZ, iii. photographic image and

	iv. other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Travel document Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier, the Personalization Agent Keys, and a unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Receiving State	The Country to which the MRTD holder is applying for entry [R18].
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R23].
skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
traveler	A person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE [R10].
Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialized and pre-personalized MRTD's chip.

User data	Data created by and for the user, that does not affect the operation of the TSF [R10].
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template [R18].
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

8.3 Technical References

[R1] ANSSI*: Rapport de certification ANSSI-CC-2012/77 Microcontroleurs securises ST23R160/80A/48A and ST23L160/80A/48A, incluant optionnellement la biblioteque cryptographique Neslib v3.1, 8 novembre 2012*

[R2] ANSSI*: Rapport de maintenance ANSSI-CC-2012/77-M01 Microcontroleurs securises ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la biblioteque cryptographique Neslib v3.1, 11 juillet 2013*

[R3] BSI: *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*

[R4] BSI: *Security IC Platform Protection Profile version 1.0 15 June, 2007; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035*

[R5] BSI: *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application ", Basic Access Control, Version 1.10, 25th March 2009, BSI-CC-PP-0055.*

[R6] BSI: *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application ", Extended Access Control with PACE, Version 1.3.2, 5th December 2012, BSI-CC-PP-0056-V2-2012.*

[R7] BSI: *Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2nd November 2011, BSI-CC-PP-0068-V2-2011.*

[R8] BSI: *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, parts 1-2-3, version 2.10, 20. March 2012*

[R9] BSI: *Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 2.00, 28 June 2012*

[R10] CCRA: *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, version 3.1 rev.4, CCMB-2012-09-001*

[R11] CCRA: *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2012, version 3.1 rev.4, CCMB-2012-09-002*

[R12] CCRA: *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2012, version 3.1 rev 4, CCMB-2012-09-003*

[R13] EMV CPS: *EMV Card Personalization Specification – version 1.0, June 2003*

[R14] Gep: *Security Target SOMA-c003 Electronic Passport, Basic Access Control" v1.0 04.03.2011.*

[R15] Gep: *Pre-personalization Guidance for SOMA-c003 electronic passport, ref. TCAE120023.*

[R16] Gep: *Personalization Guidance for SOMA-c003 electronic passport, ref. TCAE120024.*

[R17] Gep: *User Guidance for SOMA-c003 electronic passport, ref. TCAE120025.*

[R18] ICAO: *MACHINE READABLE TRAVEL DOCUMENTS – Part 3 Machine Readable Official Travel Documents, Volume 2 Specifications for Electronically Enabled MRtds with Biometric Identification Capability Approved by the Secretary General and published under his authority – Doc 9303, Third Edition – 2008*

[R19] ICAO: *SUPPLEMENT TO DOC 9303 – Release 11 – November 17, 2011*

[R20] ICAO: *TECHNICAL REPORT SUPPLEMENTAL ACCESS CONTROL FOR MACHINE READABLE TRAVEL DOCUMENTS – Version 1.01 – November 11, 2010*

[R21] ICAO: *MACHINE READABLE TRAVEL DOCUMENTS – Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability Approved by the Secretary General and published under his authority – Doc 9303, Sixth Edition – 2006*

[R22] IETF Network Working Group: *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.*

[R23] ISO/IEC: *International Standard 7816-4 2005 Information Technology – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange – January 15, 2005*

[R24] ISO/IEC: *International Standard 9796-2:2002 Information Technology – Security Techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanism, Second edition 2002-10-01*

[R25] ISO/IEC: *International Standard 9797-1 1999 Information Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*

[R26] ISO/IEC: *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics.*

[R27] ISO/IEC: *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface.*

[R28] ISO/IEC: *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.*

[R29] ISO/IEC: *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol.*

[R30] JIL: *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.*

[R31] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology*

[R32] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 186-2, DIGITAL SIGNATURE STANDARD (DSS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, January 2000*

[R33] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 180-2, SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology – 2002 August 1*

[R34] NIST: *SPECIAL PUBBLICATION 800-38B, RECOMMENDATION FOR BLOCK CIPHER MODES OF OPERATION, THE CMAC MODE FOR AUTHENTICATION, 2005*

[R35] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), 1999*

[R36] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 197, SPECIFICATION FOT THE ADVANCED ENCRYPTION STANDARD (AES), 2001*

[R37] RSA Laboratories: *PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.*

[R38] RSA Laboratories: *PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.*

[R39] STMicroelectronics: *ST23R160B, ST23R80AB, ST23R48AB, ST23L160B, ST23L80AB, ST23L48AB, all with optional cryptographic library NESLIB 3.1 Security Target – Public Version, SMD_ST23YRLxxx_ST_11_001 Rev.01.00, July 2011*

[R40] STMicroelectronics: *ST23R160 Enhanced security smartcard MCU with AES accelerator, 160-Kbyte EEPROM and dual or contact-only interface, Doc ID 022474 Rev 1, June 2012*

Appendix A   Integrated   Circuit   STMicroelectronics ST23R160/80A/48A

The following sections highlight the security features of the hardware platform ST23R160B and two commercial derivatives: ST23R80A and ST23R48A, underlying the SOMA-c003 operating system. Since the TOE trusts in and relies on the TSF of the integrated circuit, a section is dedicated to the statement of compatibility between this security target (Composite-ST) and the one of the platform (Platform-ST).

A.1   Chip Identification

The integrated circuits on which the TOE is based are the secure microcontrollers ST23R160 (master product), ST23R80A (commercial derivative) and ST23R48A (commercial derivative), all including the cryptographic library NESLIB v3.1.

According to the IC security target, "*all are based on the same hardware, the different derivatives are configured during the manufacturing process, depending on the customer order*".

The master product and the two derivatives only differ in the EEPROM size.

These chips received a Common Criteria certification at the EAL6 assurance level augmented with ALC_FLR.1 [R1][R2][R39], with certification ID:

ANSSI-CC-2012/77

The certified version of the IC is the revision B, product identification number 0019h.
The platform's certificate is valid and up-to-date.

A.2   IC Developer Identification

The developer of the ST23R160/80A/48A is STMicroelectronics.

A.3   IC Manufacturer Identification

The manufacturer of the ST23R160/80A/48A chip is STMicroelectronics.

END OF DOCUMENT