eTravel v2.0 SAC with PACE DH Security Target Lite

UPDATES

Date	Author	Modification
Jun 1st 2016	Gemalto	Creating from evaluated ST (V1.8)

CONTENT

1. ST INTRODUCTION 5

1.1 ST IDENTIFICATION 5
1.2 TOE IDENTIFICATION 5
1.3 ST OVERVIEW 7
1.4 REFERENCES 8
1.4.1 External References 8
1.4.2 Internal References 10
1.5 TOE OVERVIEW 11
1.5.1 TOE definition and operational usage 11
1.5.2 TOE boundaries 11
1.5.3 TOE major security features for operational use 13
1.5.4 TOE type 13
1.5.5 TOE life-cycle 14
1.5.5.1 Four phases 14
1.5.5.2 Actors 15
1.5.5.3 Init on module at Gemalto site 16
1.5.5.4 Init on module at Founder site 17
1.5.5.5 Init on inlay at Gemalto site 18
1.5.6 Non-TOE hardware/software/firmware 19

2. CONFORMANCE CLAIMS 20

2.1 CC CONFORMANCE CLAIM 20
2.2 PP CLAIM & CONFORMANCE STATEMENT 20
2.3 PACKAGE CLAIM 20

3. SECURITY PROBLEM DEFINITION 21

3.1 INTRODUCTION 21
3.2 THREATS 24
3.3 ORGANISATIONAL SECURITY POLICIES 27
3.4 ASSUMPTIONS 29
3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-SAC] AND [ST-IC] 29
3.5.1 Compatibility between threats of [ST-SAC] and [ST-IC] 29
3.5.2 Compatibility between OSP of [ST-SAC] and [ST-IC] 29
3.5.3 Compatibility between assumptions of [ST-SAC] and [ST-IC] 30

4. SECURITY OBJECTIVES 31

4.1 SECURITY OBJECTIVES FOR THE TOE 31
4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT 33
4.3 SECURITY OBJECTIVE RATIONALE 35
4.4 COMPATIBILITY BETWEEN OBJECTIVES OF [ST-SAC] AND [ST-IC] 37
4.4.1 Compatibility between objectives for the TOE 37
4.4.2 Compatibility between objectives for the environment 37
4.4.3 Justifications for adding objectives on the environment 37
4.4.3.1 Additions to [PP-MRTD-SAC] 37

5. EXTENDED COMPONENTS DEFINITION 38

5.1 DEFINITION OF THE FAMILY FAU_SAS 38
5.2 DEFINITION OF THE FAMILY FCS_RND 38
5.3 DEFINITION OF THE FAMILY FIA_API 39
5.4 DEFINITION OF THE FAMILY FMT_LIM 40
5.5 DEFINITION OF THE FAMILY FPT_EMS 41

6. SECURITY REQUIREMENTS 43

6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE 43
6.1.1 Overview *43*
6.1.2 Class FCS Cryptographic Support *45*
6.1.2.1 Cryptographic key generation (FCS_CKM.1) 45
6.1.2.2 Cryptographic operation (FCS_COP.1) 47
6.1.2.3 Random Number Generation (FCS_RND.1) 49
6.1.3 Class FIA Identification and Authentication *49*
6.1.4 Class FDP User Data Protection *53*
6.1.5 Class FTP Trusted Path/Channels *54*
6.1.6 Class FAU Security Audit *55*
6.1.7 Class FMT Security Management *55*
6.1.8 Class FPT Protection of the Security Functions *57*
6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE 59
6.3 SECURITY REQUIREMENTS RATIONALE 59
6.3.1 Security Functional Requirements Rationale *59*
6.3.2 Rationale for SFR's Dependencies *63*
6.3.3 Security Assurance Requirements Rationale *64*
6.3.4 Security Requirements – Internal Consistency *65*
6.3.5 Compatibility between SFR of [ST-SAC] and [ST-IC] *66*
7. TOE SUMMARY SPECIFICATION 67
7.1 TOE SECURITY FUNCTIONS 67
7.1.1 TSFs provided by the MultiApp v3 Software *67*
7.1.2 TSF provided by the M7820 chip *68*
8. GLOSSARY AND ACRONYMS 69

FIGURES

Figure 1: TOE Boundaries 12
Figure 2: LC1: Init on module at Gemalto site 16
Figure 3: LC2 Init on module at Founder site 17
Figure 4: LC3: Init on inlay at Gemalto site 18

TABLES

Table 1: Get Data on tag 0x0103 5
Table 2: Flow version byte 6
Table 2: Identification of the actors 15
Table 3: Primary assets 21
Table 4: Secondary assets 22
Table 5: Subjects and external entities 24
Table 6: Security Objective Rationale 35
Table 7: Security functional groups vs. SFRs 44
Table 8: Keys and Certificates 44
Table 9: FCS_CKM.1/DH_PACE refinements 45
Table 10: FCS_CKM.1/KeyPair refinements 46
Table 11: FCS_CKM.1/PERSO refinements 46
Table 12: FCS_COP.1/PACE_ENC refinements 47
Table 13: FCS_COP.1/PACE_MAC refinements 47
Table 14: FCS_COP.1/PERSO refinements 48
Table 15: FCS_COP.1/AA refinements 48
Table 16: Overview of authentication SFR 49
Table 17: FIA_AFL.1/PACE refinements 49
Table 18: FIA_AFL.1/PERSO refinements 50

Table 19: FPT_TST refinements 59
Table 20: Coverage of Security Objectives for the TOE by SFR 60
Table 21: SFR dependencies rationale 64
Table 22: SAR Dependencies 65
Table 23: Security Functions provided by the MultiApp v3 Software 67
Table 24: Security Functions provided by the M7820 chip 68

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	eTravel v2.0 SAC with PACE DH Security Target
Version:	1.8p
ST reference:	D1392953
Origin:	Gemalto
Product identification:	eTravel SAC/EAC/BAC V2.0 with Filter 5.0 on MultiApp V3
Security Controllers:	M7820 A11
TOE identification:	Etravel EAC V2.0 & SAC (DH)
TOE documentation:	Operational User Guidance [OPE_MRTD] Preparative procedures [PRE_MRTD]

1.2 TOE IDENTIFICATION

The TOE is identified by a Get Data command on tag 0x0103.

Group	Byte	Description	Value	Length	Identifies:
R&D	00	Gemalto Family Name – Javacard	**B0h**	1	OS
	01	Gemalto OS name – MultiApp ID	**85h**	1	OS
	02	Gemalto Mask Number – G260	**43h**	1	OS
	03	Gemalto Product Name: MultiApp ID v3.0 Combi 160K	**3Fh**	1	OS
	04	Gemalto Flow version	**41h**	1	Application type and configuration
	05	Gemalto Filter Set – Filter V5.0	**50h**	1	Filter
	06	Chip Manufacturer – Infineon	**4090h**	2	IC
	08	Chip Version – SLE78CLX1600P	**7164h**	2	IC
	10	Submask identifier - OBKG/Patch/BPU infos (80K for customer memory)	**0050h**	2	Configuration
	12	TP Identifier of the product	**0335500000000000h**	7	OS and Application
Personnalization	xxh	**To Be completed by init team**	-	0Bh	

Table 1: Get Data on tag 0x0103

Byte no. 04 Gemalto Flow version

This byte refers to the type of the existing application on the product. In this case, the value 41h, refers to an eTravel type of application.

Gemalto Flow version byte								
Description	***MSB***				***LSB***			
Flow version	X	x	x	x	0	0	0	1
init is compliant with the config PPSUN	x	x	x	1				
init is compliant with the config PPSCD	x	x	1	x				
init is compliant with the config eTravel	x	1	x	x				

Table 2: Flow version byte

Byte no. 12 TP Identifier of the product

This byte's value refers to the complete TOE identification on the Product Identification and Lifecycle management data base from Gemalto. The value refers to the Technical Product (**T1033550**) which in this case its description on the database is the following:

> Existing MultiApp ID V3.0 PACE DH product (T1025786 B)
> with IAS ECCv4 application on top of it.
>
> IAS ECC v4 optimized binaries are used.
>
> This TP is specifically created for the PPSAC Close Configuration (= not possible to load any applet afterwards)

Together Byte no. 04 and Byte no.12 gives the CLOSED attribute configuration to the product.

> The TOE and the product differ, as further explained in TOE Overview.

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command.

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless based communication according to [ISO14443].
From the logical point of view, the TOE shall be able to recognise the following terminal type, which, hence, shall be available: – Basic Inspection System with PACE.
The TOE shall require terminals to evince possessing authorisation information (a shared secret) before access according to [ICAO-TR-SAC], option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.
In scope of this Protection Profile the following types of inspection systems shall be distinguished (for a more detailed description see Glossary):

- BIS-PACE: Basic Inspection System with PACE,

- BIS-BAC: Basic Inspection System with BAC,

The current ST defines security policy for the usage of only Basic Inspection System with PACE (BIS-PACE) in the context of the ePassport application. Using other types of inspection systems and terminals is out of the scope of the current ST. In order to be downwardly compatible with ICAO-terminals, this product also functionally supports Basic Access Control (BAC). However, using BAC is not conformant to the current ST; it is conformant to [ST_BAC]. When performing BAC, the TOE is acting outside of security policy defined by the current ST. Therefore, organisations being responsible for the operation of inspection systems shall be aware of this context.

Application note: A terminal shall always start a communication session using PACE. If successfully, it should then proceed with passive authentications. If the trial with PACE failed, the terminal may try to establish a communication session using other valid options as described above.

1.3 ST OVERVIEW

The ST is based on Protection Profile *Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control* [PP-MRTD-SAC].
The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) based on the requirements of the International Civil Aviation Organization (ICAO). More specifically the TOE consists of operating system of MRTD's chip with ICAO application. The TOE is programmed according to Logical Data Structure as defined in [ICAO-9303]. This TOE can be integrated in secure document booklet or can also be provided in ID-1 card.

This Security Target defines the security requirements for the TOE. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the MRTD application and data during its life cycle.

The Multiapp V3 product is an open platform [ST-Platform] in closed configuration preventing to load applications during operational phase.

The main objectives of this ST are:

- To introduce TOE and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

1.4 REFERENCES

1.4.1 External References

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 4, September 2012
[RGS-B1]	Referentiel general de sécurité version 1.0 Annexe B1 Mechanismes cryptographiques…version 1.20 du 26 Janvier 2010
[ST-IC]	Either [ST-IC-M7820]
[ST-IC-M7820]	ST of M7820 A11 SLE78CLX1600P - Rev. 0.6 - 28 August 2012
[CR-IC]	Either [CR-IC-M7820]
[CR-IC-M7820]	Certification Report, BSI-DSZ-CC-0829-2012 (05-09-2012)
[FIPS180-2]	*Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+Change Notice to include SHA-224),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[FIPS46-3]	*Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, Reaffirmed 1999 October 25
[ISO15946-1]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002
[ISO15946-2]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures, 2002
[ISO15946-3]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002
[ISO7816]	ISO 7816, Identification cards – Integrated circuit(s) cards , Version Second Edition, 2008
[ISO9796-2]	ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002
[ISO9797-1]	ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 1999

[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ICAO-9303]	9303 Part 3 Vol 2 – ICAO Machine Readable Travel Document Third edition 2008
[ICAO-TR-SAC]	ICAO TR –Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, March 23, 2010
[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	*MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access* International Civil Aviation Organization Version 1.1, October 01 2004
[PP-IC-0035]	*Smartcard IC Platform protection Profile* BSI-PP-0035
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03M01, Version 3.0, May 2012
[PP-MRTD-EAC]	Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP) BSI-CC-PP-0056-V2-2012 (Version 1.3.1, 22th March 2012)
[PP-MRTD-SAC]	Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011
[PP-MRTD-BAC]	Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC PP) BSI-PP-0055, version 1.10, 25th March 2009
[Sec-9303]	*ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS*, *Excerpts from ICAO Doc 9303, Part 1* Machine Readable Passports, Fifth Edition – 2003
[TR-EAC-1]	Technical Guideline – TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012
[TR-ECC]	Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, BSI, 17.04.2009
[BIO]	BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004
[IAS ECC]	EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS IAS ECC Identification Authentication Signature European Citizen Card, Technical Specifications Revision: 1.0.1, 23/02/2009
[IEEE-P1363]	Standard Specifications for Public-Key Cryptography

1.4.2 Internal References

[ST-EAC]	D1392954 EAC Security Target - CAPRI: eTravel v2.0 EAC with PACE DH Security Target
[ST-SAC]	D1392953 SAC Security Target - CAPRI: eTravel v2.0 SAC with PACE DH Security Target
[ST-BAC]	D1392955 BAC Security Target - CAPRI: eTravel v2.0 BAC with PACE DH Security Target
[PRE_MRTD]	D1191507 Preparative procedures - MultiApp V3 MRTD CYLLENE3
[OPE_MRTD]	D1191508 Operational User Guidance - MultiApp V3 MRTD CYLLENE3
[ST-Platform]	D1184308 JCS Security Target - MultiApp V3 CYLLENE3

1.5 TOE OVERVIEW

1.5.1 TOE definition and operational usage

The Target of Evaluation (TOE) addressed by the current ST is an electronic travel document representing a contactless / contact smart card[1] programmed according to ICAO Technical Report "Supplemental Access Control" [ICAO-TR-SAC].

This smart card / passport provides the following mechanisms:

- the Basic Access Control (BAC) according to the ICAO document [PKI]
- the Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]
- the Supplemental Access Control (SAC) according to the ICAO document [ICAO-TR-SAC]
- the Extended Access Control (EAC) according to the BSI document [TR-EAC-1]

Application note: SAC will eventually replace BAC. In this transition period, and for legacy reasons, MultiApp v3 also supports BAC when it is connected to a BIS.

Application note: Additionally to the [PP-MRTD-SAC], the TOE has a set of administrative commands for the management of the product during the product life.

For the *ePassport* application, the travel document holder can control access to his user data by conscious presenting his travel document to governmental organisations[2].
The travel document's chip is integrated into a physical (plastic or paper), optically readable part of the travel document, which – as the final product – shall eventually supersede still existing, merely optically readable travel documents. The plastic or paper, optically readable cover of the travel document, where the travel document's chip is embedded in, is not part of the TOE. The tying-up of the travel document's chip to the plastic travel document is achieved by physical and organisational security measures being out of scope of the current ST.

The TOE comprises:

i) the circuitry of the contactless chip incl. all IC dedicated software[3] being active in the operational phase of the TOE (the integrated circuit, IC). The contact interface has been disabled.
ii) the IC Embedded Software (operating system)[4],
iii) the *ePassport* application and
iv) the associated guidance documentation.

1.5.2 TOE boundaries

Application note: Components within the TOE boundary are refined in the following manner:

- *the Integrated Circuit (IC),*
- *the IC Dedicated Test Software,*
- *the IC Dedicated Support Software (Boot Rom Software, Operating System),*
- *the eTravel EAC on MultiApp v3 Embedded Software (ES),*
- *the NVM Embedded Software,*
- *part of the MRTD Logical Data Structure,*
- *the guidance documentation of the eTravel EAC on MultiApp v3 product:*
  - *the preparation guide (assurance family AGD-PRE),*
  - *the operational guide (assurance family AGD-OPE).*

[1] maybe also contained in a booklet
[2] 4 CAN or MRZ user authentication, see [ICAO-TR-SAC]
[3] usually preloaded (and often security certified) by the Chip Manufacturer
[4] usually – together with IC – completely implementing executable functions

The eTravel EAC on MultiApp v3 Embedded Software (ES) is implemented in the ROM of the chip.
As part of the delivered product to the customer, there is the **IAS ECCv4** application, commonly known as ***IAS ECC 1.0.1*** as for the conformance to the IAS ECC, *Identification Authentication Signature European Citizen Card, Technical Specifications Revision 1.0.1* [IAS ECC]. This application is NOT part of the TOE.

The IAS ECCv4 application is identified with the following information:

IASECC Applet, Instance application AID: **A0000000308000000009816001**

Get Data, Tag 4F4A information:
Applet Version : **4.3.2.A**

MKS Information:
Build date: **5/08/2015**

Checkpoint: **1.233**

Label: **IDApplets.IASECCv4onMAV30.ReleaseCandidate.002**

Below is an overview of the product with the TOE boundaries, TSF and non-TSF parts.

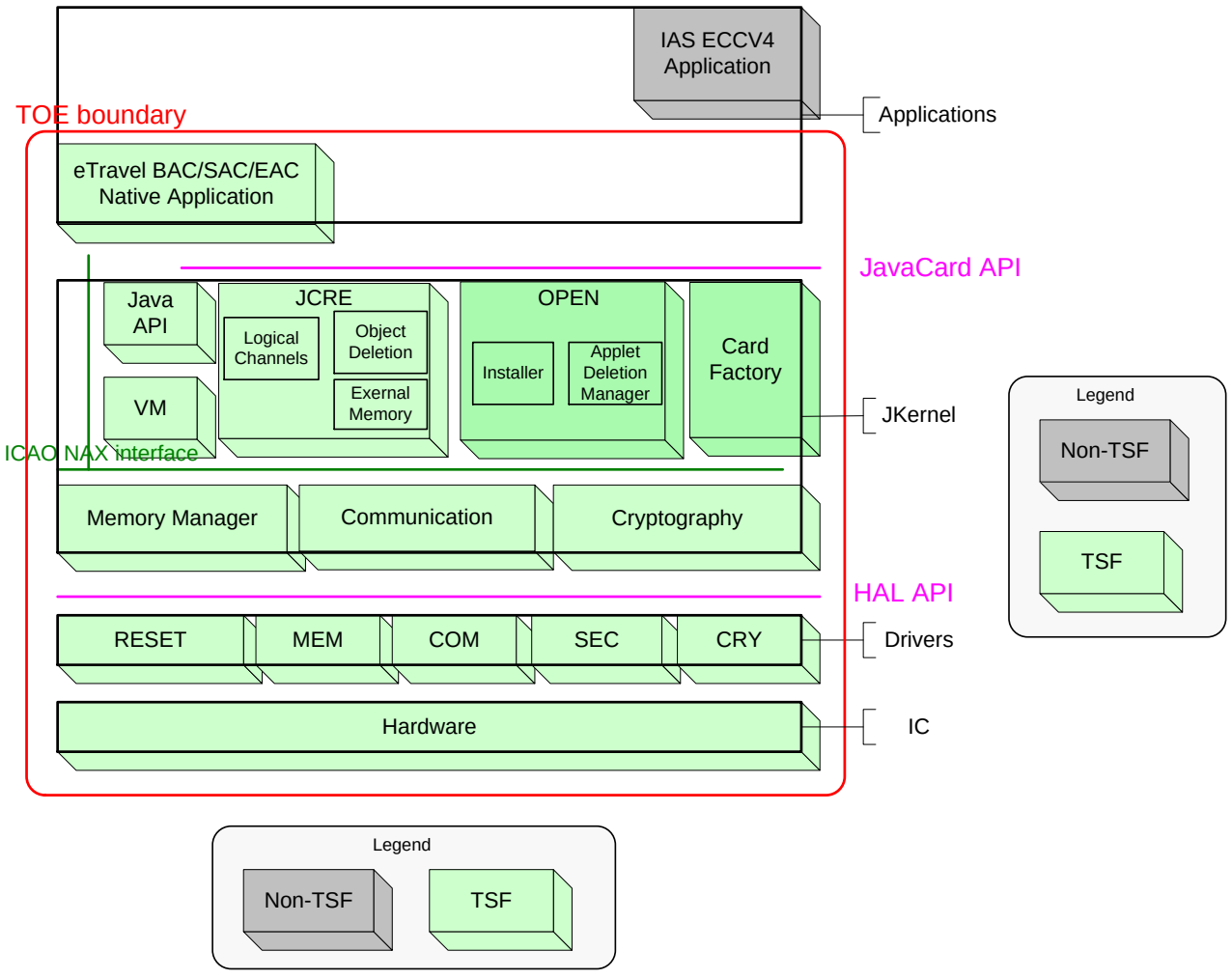


Figure 1: TOE Boundaries

1.5.3 TOE major security features for operational use

The following TOE security features are the most significant for its operational use:

- Only terminals possessing authorisation information (the shared secret may be CAN or MRZ optically retrieved by the terminal, or a confidential PIN) can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the terminal connected[5],
- Averting of inconspicuous tracing of the travel document,
- Self-protection of the TOE security functionality and the data stored inside.

1.5.4 TOE type

The TOE type is contactless/contact smart card with the *ePassport* application named as a whole 'travel document'.

The typical life cycle phases for the current TOE type are development[6], manufacturing[7], card issuing[8] and, finally, operational use. Operational use of the TOE is explicitly in the focus of this ST. Some single properties of the manufacturing and the card issuing life cycle phases being significant for the security of the TOE in its operational phase are also considered by the current PP. A security evaluation/certification being conform with this PP will have to involve all life cycle phases into consideration to the extent as required by the assurance package chosen here for the TOE (see 2.3 Package Claim).

[5] inspecting official organisation is technically represented by a local RF-terminal as the end point of secure communication in the sense of this PP (local authentication)
[6] IC itself and IC embedded software
[7] IC manufacturing and smart card manufacturing including installation of a native card operating system
[8] including installation of the smart card application(s) and their electronic personalisation (i.e. tying the application data up to the travel document holder)

1.5.5 TOE life-cycle

1.5.5.1 Four phases

The TOE life cycle is described in terms of the four life cycle phases. With respect to [PP-BSI-0035], the TOE life cycle is additionally subdivided into 7 steps.

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the 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.

Phase 2 “Manufacturing”:
(Step3) In a first step the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software and the parts of the travel document’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacture to the travel document manufacturer.
If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

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

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

Application note: Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF
- For JavaCard operating systems: the Applet instantiation.

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.

Phase 3 “Personalization of the travel document”:
(Step6) 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 printing 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 [PKI] 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 travel document holder for operational use.

Phase 4 “Operational Use”
(Step7) The TOE is used as a travel document's chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

1.5.5.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	IFX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	IFX
Initializer	Gemalto or IFX
Pre-personalizer	Gemalto or IFX
Inlay manufacturer	Gemalto or another Inlay manufacturer
Book manufacturer	Gemalto or another printer
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 3: Identification of the actors

1.5.5.3 *Init on module at Gemalto site*

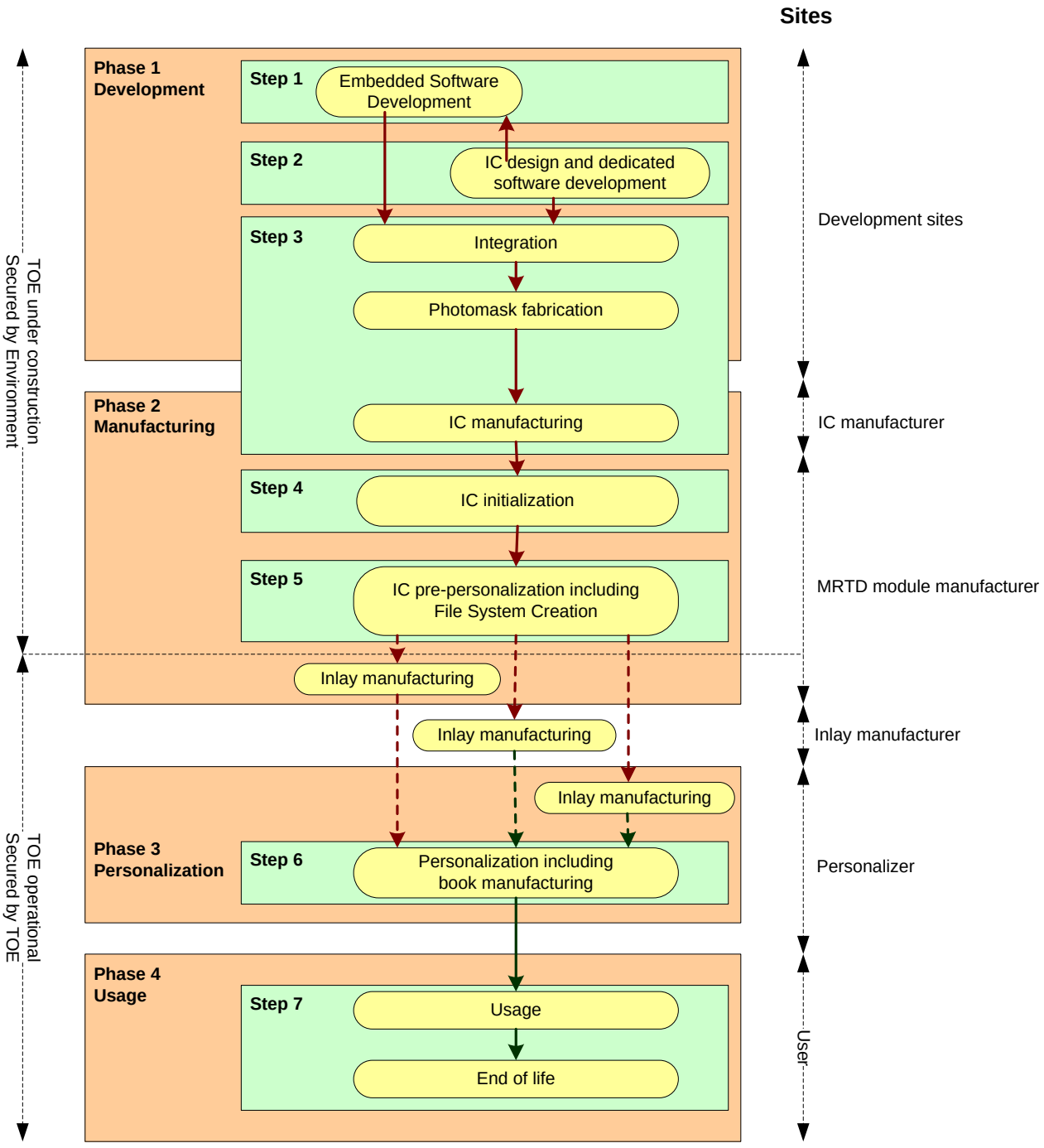


Figure 2: LC1: Init on module at Gemalto site

Figure 2: LC1: Initialization on module at Gemalto site describes the standard Life Cycle. The IC is manufactured at the founder site. It is then shipped to Gemalto site where it is initialized/pre-personalized. The transformation of wafers into modules can be performed either at the founder site or at Gemalto site. The modules are then shipped to the Personalizer or to the Inlay manufacturer. In the latter case, The Inlay manufacturer ships the inlays to the Personalizer
During the shipment from Gemalto to the Personalizer or the Inlay manufacturer, the module is protected by a diversified key.

1.5.5.4 *Init on module at Founder site*

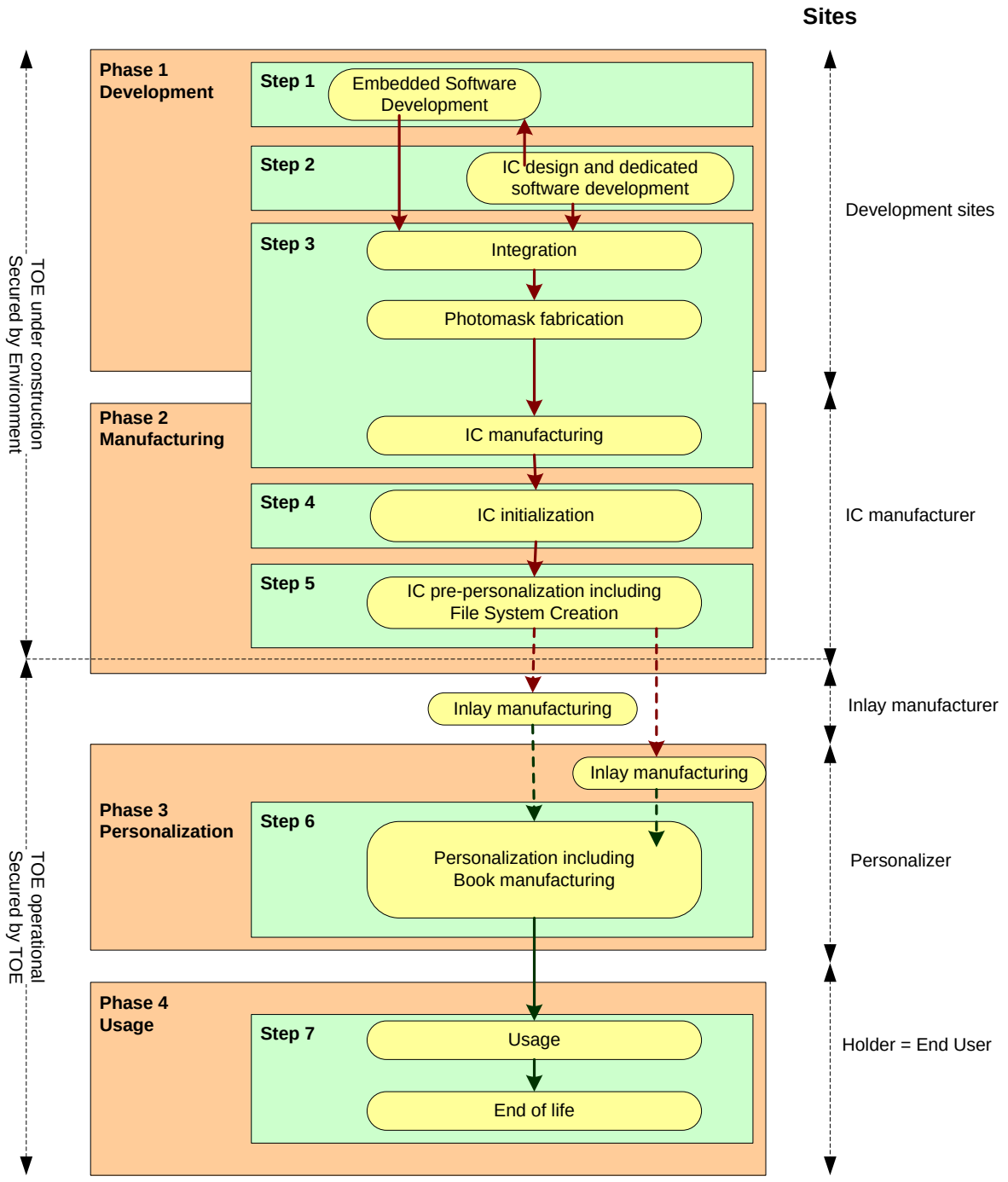


Figure 3: LC2 Init on module at Founder site

LC2 is an alternative to LC1. *Figure 3: LC2 Init on module at Founder site* describes the Life Cycle when the customer wishes to receive wafers directly from the founder. In this case, initialization and pre-personalization, which include sensitive operations such as the loading of patches, take place at the founder site. The creation of files is started by the founder and completed by the personalizer.
During the shipment from the founder to the Personalizer, the module is protected by a diversified key.

1.5.5.5 *Init on inlay at Gemalto site*

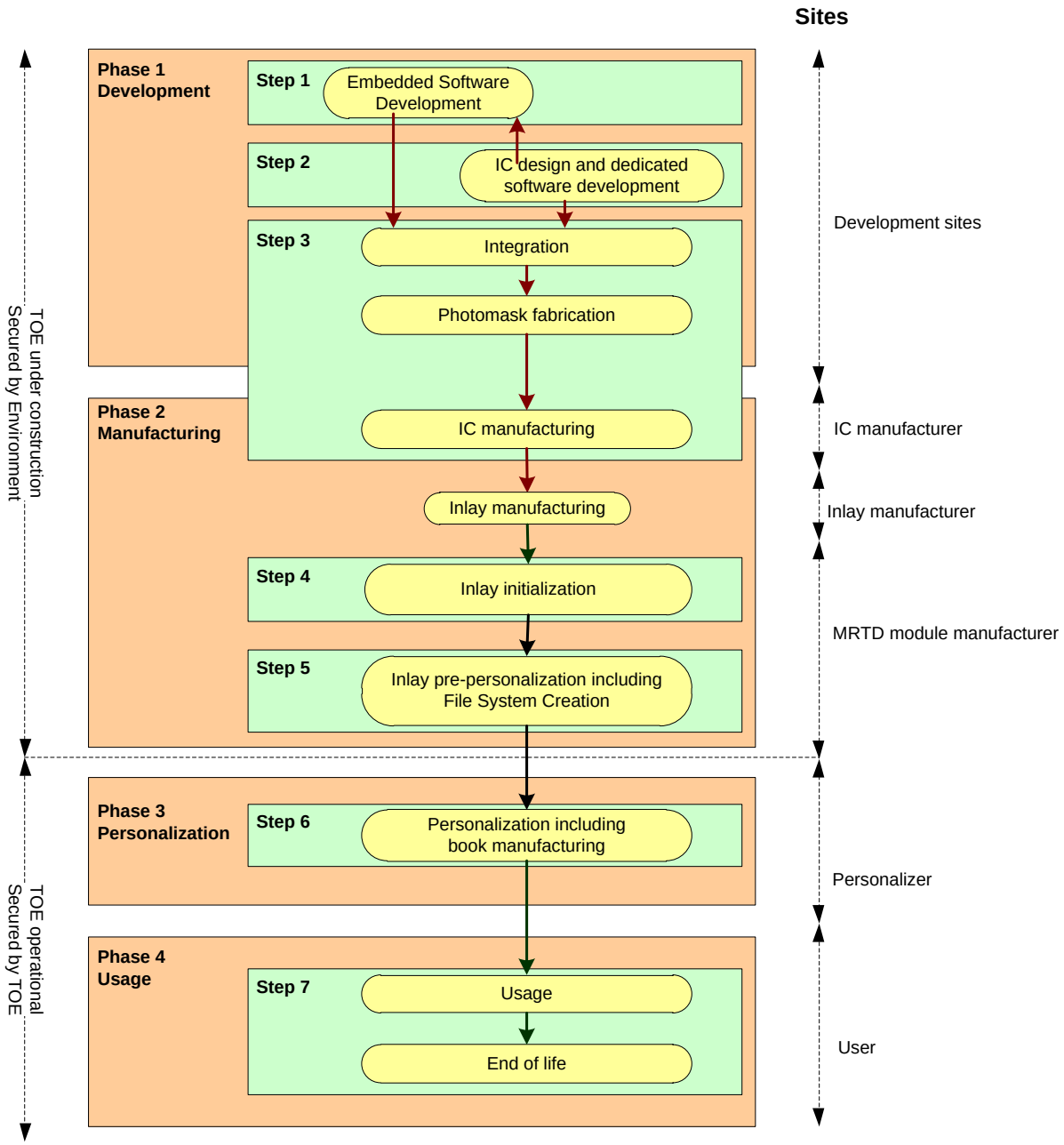


Figure 4: LC3: Init on inlay at Gemalto site

LC3 is another alternative to LC1. *Figure 4: LC3: Init on inlay at Gemalto site* describes the Life Cycle when Gemalto wishes to receive inlays instead of modules. In this case, the founder ships the module to the Inlay manufacturer.
During the shipment from the founder to Gemalto, the module is protected by a diversified key.

1.5.6 Non-TOE hardware/software/firmware

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless based communication according to [ISO14443].
From the logical point of view, the TOE shall be able to recognise the following terminal type, which, hence, shall be available: – Basic Inspection System with PACE.
The TOE shall require terminals to evince possessing authorisation information (a shared secret) before access according to [ICAO-TR-SAC], option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.
In scope of this Protection Profile the following types of inspection systems shall be distinguished (for a more detailed description see Glossary):

- BIS-PACE: Basic Inspection System[9] with PACE[10],
- BIS-BAC: Basic Inspection System with BAC[11],

The current ST defines security policy for the usage of only Basic Inspection System with PACE (BIS-PACE) in the context of the ePassport application. Using other types of inspection systems and terminals is out of the scope of the current ST. In order to be downwardly compatible with ICAO-terminals[12], this product also functionally supports Basic Access Control (BAC). However, using BAC is not conformant to the current ST; it is conformant to [ST_BAC]. When performing BAC, the TOE is acting outside of security policy defined by the current ST. Therefore, organisations being responsible for the operation of inspection systems shall be aware of this context.

Application note: A terminal[13] shall always start a communication session using PACE. If successfully, it should then proceed with passive authentications. If the trial with PACE failed, the terminal may try to establish a communication session using other valid options as described above.

[9] a Basic Inspection Systems always uses Standard Inspection Procedure
[10] SIP with PACE means: PACE and passive authentication with SO_D
[11] SIP with BAC means: BAC and passive authentication with SO_D. It is commensurate with BIS in [9] ; i.e. the terminal proven the possession of MRZ optically read out from the plastic part of the card.
[12] so called non-compliant inspection systems not supporting PACE
[13] see [4] for further details

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to be taken into account.

2.2 PP CLAIM & CONFORMANCE STATEMENT

The MultiApp v3 SAC security target claims strict conformance to [PP-MRTD-SAC].

The TOE also claims conformance to other Protection Profiles. This is described in other Security Targets:

- The MultiApp v3 EAC security target claims strict conformance to [PP-MRTD-EAC].
- The MultiApp v3 BAC security target claims demonstrable conformance to [PP-MRTD-BAC].

2.3 PACKAGE CLAIM

This ST is conformant to the following security requirements package:

- Assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-3].

3. SECURITY PROBLEM DEFINITION

3.1 INTRODUCTION

Assets
The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap. 8 Glossary for the term definitions)

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 [ICAO-TR-SAC] and being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [PP-MRTD-BAC].	Confidentiality[14] Integrity Authenticity
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 [ICAO-TR-SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). User data can be received and sent (exchange Û {receive, send}).	Confidentiality[15] 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 PAC E password. TOE tracing data can be provided / gathered.	unavailability[16]

Table 4: Primary assets

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

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

[14] Though not each data element stored on the TOE represents a secret, the specification [ICAO-TR-SAC] anyway requires securing their confidentiality: only terminals authenticated according to [ICAO-TR-SAC] can get access to the user data stored. They have to be operated according to P.Terminal.
[15] Though not each data element being transferred represents a secret, the specification [ICAO-TR-SAC] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [ICAO-TR-SAC].
[16] represents a prerequisite for anonymity of the travel document holder

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 [PP-MRTD-BAC].	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 non-secret material (Document Security Object SOD 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[17] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

Table 5: Secondary assets

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

Subjects and external entities

This security target considers the following external entities and subjects:

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[18]. This entity is commensurate with 'MRTD Holder' in [9]. Please note that a travel document holder can also be an attacker (s. below).
2	-	travel document presenter (traveller)	A person presenting the travel document to a terminal[19] and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [9]. Please note that a travel document presenter can also be an

[17] The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.
[18] i.e. this person is uniquely associated with a concrete electronic Passport
[19] in the sense of [4]

External Entity No.	Subject No.	Role	Definition
			attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [9].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[20] and verifying the travel document presenter as the travel document holder (for *ePassport*: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. See also par. 1.2.5 above.
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 [PKI]. This role is usually delegated to a Personalisation Agent.
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 be distributed by strictly secure diplomatic means, see. [PKI], 5.5.1.
7	4	Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [ST-BAC].
8	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC

[20] concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase[21]. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [ST-BAC].
9	-	Attacker	A threat 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 with 'Attacker' in [ST-BAC].

Table 6: Subjects and external entities[22]

3.2 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 assets protected by the TOE and the method of TOE's use in the operational environment.
The following threats are defined in the current PP (they are initially derived from the ICAO-BAC PP [PP-MRTD-BAC] and ICAO-EAC PP [PP-MRTD-EAC]):

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: When using BIS-BAC MultiApp v3 cannot avert this threat in the context of the security policy defined in this ST.

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

[21] cf. also par. 1.2.3 in sec. 1.2.3 above
[22] This table defines external entities and subjects in the sense of [CC-1] . Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC-1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE.

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: When using BIS-BAC MultiApp v3 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: This Threat completely covers and extends “T.Chip-ID” from [ST--BAC].

Application Note: When using BIS-BAC MultiApp v3 cannot avert this threat in the context of the security policy defined in this PP, see also §1.5.6 above.

Application Note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document’s chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document)[23] 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

[23] Such a threat might be formulated like: ‘An attacker produces an unauthorised copy or reproduction of a *genuine* travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of 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 legitimate travel documents
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document

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

T.Information_Leakage Information Leakage from travel document

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

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

T.Phys-Tamper Physical Tampering

Adverse action:	An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.
Threat agent:	high attack potential, being in possession of one or more legitimate travel documents
Asset:	integrity and authenticity of the travel document, availability of the functionality

of the travel document, confidentiality of User Data and TSF-data of the travel document

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

T.Malfunction Malfunction due to Environmental Stress

Adverse action:	An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent:	having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation
Asset:	integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

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

3.3 ORGANISATIONAL SECURITY POLICIES

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

P.Manufact Manufacturing of the travel document's chip

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

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

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

2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE[24].

[24] cf. Table 4 and Table 5 above

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

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

P.Card_PKI PKI for Passive Authentication (issuing branch)

Application Note 20: 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 [PKI] , 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 [PKI], 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 Trustworthiness of PKI

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

P.Terminal Abilities and trustworthiness of terminals

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

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

2.) They shall implement the terminal parts of the PACE protocol [ICAO-TR-SAC], of the Passive Authentication [PKI] and use them in this order[25]. 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.

[25] This order is commensurate with [ICAO-TR-SAC].

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, [PKI]).

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.Activ_Auth Active Authentication

The TOE implements the active authentication protocol as described in [ICAO-9303].

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

3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-SAC] AND [ST-IC]

3.5.1 Compatibility between threats of [ST-SAC] and [ST-IC]

T.Skimming, T.Eavesdropping, T.Tracing are specific to the Java Card platform and they do no conflict with the threats of [ST-IC].
T.Forgery is included in T.Phys-Manipulation.
T.Abuse-Func of [ST-SAC] is included in T.Abuse-Func of [ST-IC].
T.Information_Leakage is included in T.Leak-Inherent and T.Leak-Forced.
T.Phys-Tamper is included in T.Phys-Manipulation
T.Malfunction of [ST-SAC] is included in T.Malfunction of [ST-IC].

We can therefore conclude that the threats of [ST-SAC] and [ST-IC] are consistent.

3.5.2 Compatibility between OSP of [ST-SAC] and [ST-IC]

P.Manufact, P.Pre-Operational**,** P.Card_PKI, P.Trustworthy_PKI, P.Terminal and P.Active_Auth are specific to the MRTD and they do no conflict with the OSP of [ST-IC].

We can therefore conclude that the OSP of [ST-SAC] and [ST-IC] are consistent.

3.5.3 Compatibility between assumptions of [ST-SAC] and [ST-IC]

A.Passive_Auth is assumption specific to [ST-SAC] and they do no conflict with the assumptions of [ST-IC].

We can therefore conclude that the assumptions for the environment of [ST-SAC] and [ST-IC] are consistent.

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

The following TOE security objectives address the protection provided by the TOE *independent* of TOE environment.

OT.Data_Integrity Integrity of Data
The TOE must ensure integrity of the User Data and the TSF-data[26] 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[27] stored on it by enabling verification of their authenticity at the terminal-side[28].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)[29].

OT.Data_Confidentiality Confidentiality of Data
The TOE must ensure confidentiality of the User Data and the TSF-data[30] by granting read access only to the PACE authenticated BIS-PACE connected.The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

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

Application note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)[31] cannot be achieved by the current TOE.

OT.Prot_Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to

[26] where appropriate, see Table 5 above
[27] where appropriate, see Table 5 above
[28] verification of SO_D
[29] secure messaging after the PACE authentication, see also [ICAO-TR-SAC]
[30] where appropriate, see Table 5 above
[31] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [PKI] '.

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 or/and TSF-data stored and/or processed by the travel document

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

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

OT.Prot_Phys-Tamper Protection against Physical Tampering

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

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

with a prior

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

OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

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

OT.Identification Identification of the TOE

The TOE must provide means to store Initialisation[32] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and

[32] amongst other, IC Identification data

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 Personalisation of logical MRTD

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

Application note: The OT.AC_Pers implies that 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.Activ_Auth_Proof Proof of MRTD's chip authenticity through AA

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

4.2 SECURITY OBJECTIVES FOR 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:

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 [PKI]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [PKI]. 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 [PKI][33], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [PKI] (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 [PKI].

2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-SAC], of the Passive Authentication [ICAO-TR-SAC] (by verification of the signature of the Document Security Object) and use them in this order[34]. 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, [PKI]).

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

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.

OE.Active_Auth_Sign Active Authentication of logical MRTD by Signature

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

OE.Active_Auth_Verif Verification by Active Authentication

[33] see also [PKI] , sec. 10
[34] This order is commensurate with [ICAO-TR-SAC].

In addition to the verification by passive authentication, the inspection systems may use the verification by active authentication, which offers a stronger guaranty of the authenticity of the MRTD.

4.3 SECURITY OBJECTIVE RATIONALE

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and *necessity* of the objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	OT.Identification	OT.AC_Pers	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_Malfuntion	OT.Activ_Auth_Proof	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Skimming			X	X	X										X			
T.Eavesdropping					X													
T.Tracing						X									X			
T.Forgery		X	X	X			X		X		X	X	X	X			X	X
T.Abuse-Func							X											
T.Information_Leakage								X										
T.Phys-Tamper									X									
T.Malfunction										X								
P.Manufact	X																	
P.Pre-Operational	X	X										X				X		
P.Terminal														X				
P.Card_PKI													X					
P.Trustworthy_PKI													X					
P.Active_Auth											X						X	X
A.Passive_Auth													X					

Table 7: Security Objective Rationale

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. ". The TOE environment will also detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active_Auth_Sign "**Active Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Active_Auth_Verif** "Verification by Active Authentication". This is possible only because genuine TOE enforce AA as specified in **OT.Activ_Auth_Proof**.

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.

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 OSP **P.Activ_Auth** is enforced by the AA protocol as specified in **OT.Activ_Auth_Proof**. In addition the TOE environment will also detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active_Auth_Sign "**Active Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Active_Auth_Verif** "Verification by Active Authentication".

The assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** “Authentication of travel document by Signature” .

4.4 COMPATIBILITY BETWEEN OBJECTIVES OF [ST-SAC] AND [ST-IC]

4.4.1 Compatibility between objectives for the TOE

OT.AC_Pers and OT.Tracing are specific to [ST-SAC] and they does no conflict with the objectives of [ST-IC].
OT.Data_Integrity and OT.Data_Authenticity are included in O.Phys-Manipulation.
OT.Data_Confidentiality is specific to [ST-SAC] and it does no conflict with the objectives of [ST-IC].
OT.Identification is included in O.Identification.
OT.Chip_Auth_Proof is specific to [ST-SAC] and it does no conflict with the objectives of [ST-IC].
OT.Prot_Abuse-Func is included in O.Abuse-Func.
OT.Prot_Inf_Leak is included in O.Leak-Inherent and O.Leak-Forced
OT.Prot_Phys-Tamper is included in O.Phys-Manipulation.
OT.Prot_Malfunction is included in O.Malfunction.
OT.Activ_Auth_Proof is specific to [ST-SAC] and it does no conflict with the objectives of [ST-IC].

We can therefore conclude that the objectives for the TOE of [ST-SAC] and [ST-IC] are consistent.

4.4.2 Compatibility between objectives for the environment

OE.MRTD_Manufact is included in OE.Process-TOE and OE.Process-Card.
OE.MRTD_ Delivery is included in OE.Process-Card.
OE.Personalization is partly included in OE.Process-Card.
OE.Pass_Auth_Sign, OE.Auth_Key_MRTD, OE.Authoriz_Sens_Data, OE.BAC_PP, OE.Exam_MRTD, OE.Passive_Auth_Verif, OE.Prot_Logical_MRTD, and OE.Ext_Insp_Systems are specific to [ST-SAC] and they do no conflict with the objectives of [ST-IC].
OE.Active_Auth_Sign and OE.Active_Auth_Verif are specific to [ST-SAC] and they do no conflict with the objectives of [ST-IC].
We can therefore conclude that the objectives for the environment of [ST-SAC] and [ST-IC] are consistent.

4.4.3 Justifications for adding objectives on the environment

4.4.3.1 Additions to [PP-MRTD-SAC]

The only additional objectives on the environment are OE.Active_Auth_Sign and OE.Active_Auth_Verif. These objectives request the environment to support Active Authentication. AA is an operation outside [PP-MRTD-SAC]. Therefore the added objectives on the environment do not weaken the TOE.

5. EXTENDED COMPONENTS DEFINITION

This protection profile uses components defined as extensions to CC part 2. Most of them are drawn from [11].

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.

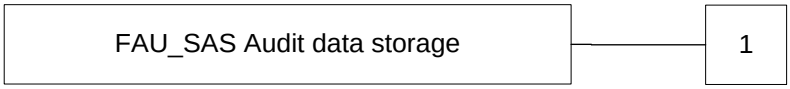
The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behavior

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

Component leveling



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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised 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:

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:

FCS_RND Generation of random numbers	1

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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1Quality 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 IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

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

Component levelling:

FIA_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

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

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies

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

5.4 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.

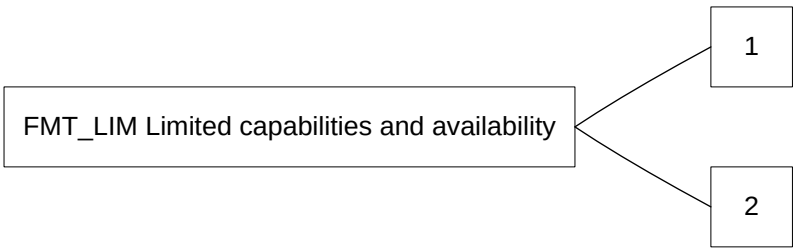
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

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 access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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

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

or conversely

(ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the 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 [CC-2].

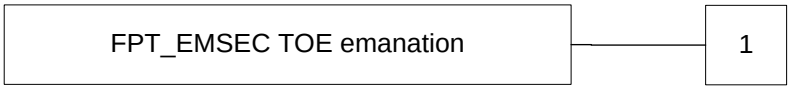
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6. SECURITY REQUIREMENTS

6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

6.1.1 Overview

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.
Refinements in this section are in underline font when the SFR's refinement is already present in [PP-MRTD-SAC], and in bold font when the refinement is done in this ST. When the SFR is refined in the [PP-MRTD-SAC] and additionally refined in this ST then the font is bold and underline.

In order to give an overview of the security functional requirements in the context of the security services offered by the TOE, the author of [PP-MRTD-SAC] defined the security functional groups and allocated the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Access control to the User Data stored in the TOE	– {FDP_ACC.1/TRM, FDP_ACF.1/TRM} Supported by: – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)
Secure data exchange between the travel document and the terminal connected	– FTP_ITC.1/PACE: trusted channel Supported by: – FCS_COP.1/PACE_ENC: encryption/decryption – FCS_COP.1/PACE_MAC: MAC generation/verification – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE)
Identification and authentication of users and components	– FIA_UID.1/PACE: PACE Identification (PACE authenticated BIS-PACE) – FIA_UAU.1/PACE: PACE Authentication (PACE authenticated BIS-PACE) – FIA_UAU.4/PACE: single-use of authentication data – FIA_UAU.5/PACE: multiple authentication mechanisms – FIA_UAU.6/PACE: Re-authentication of Terminal – FIA_AFL.1/PACE: reaction to unsuccessful authentication attempts for establishing PACE communication using *non-blocking* authentication and authorisation data Supported by: – FCS_CKM.1/DH_PACE: PACE authentication (PACE authenticated BIS-PACE) – FCS_CKM.4: session keys destruction (authentication expiration) – FCS_RND.1: random numbers generation – FMT_SMR.1/PACE: security roles definition.
Audit	– FAU_SAS.1: Audit storage Supported by: – FMT_MTD.1/INI_ENA: Writing Initialisation and Pre-personalisation – FMT_MTD.1/INI_DIS: Disabling access to Initialisation and Pre-personalisation Data in the operational phase
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by:

Security Functional Groups	Security Functional Requirements concerned
	– the entire class FIA: user identification / authentication
Accuracy of the TOE security functionality / Self-protection	– The entire class FPT – FDP_RIP.1: enforced memory/storage cleaning Supported by: – the entire class FMT.

Table 8: Security functional groups vs. SFRs

The following table provides an overview of the keys and certificates used for enforcing the security policy defined in the current PP:

Name	Data
Receiving PKI branch	
	No receiving PKI branch is necessary for the current TOE due to applying Standard Inspection Procedure
Issuing PKI branch	
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. [PKI], 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}).
Session keys	
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 [ICAO-TR-SAC].
Ephemeral keys	
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 for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3

Table 9: Keys and Certificates

6.1.2 Class FCS Cryptographic Support

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

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]: fulfilled by **FCS_COP.1/PACE_ENC** and **FCS_COP.1/PACE_MAC**
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 [selection: *Diffie-Hellman-Protocol compliant to [PKCS#3]*] and specified cryptographic key sizes **Table 10 column Key size** bit that meet the following: [ICAO-TR-SAC].

iteration	Algorithm	Key size
/SKPICC-DH	**DH Key Agreement Algorithm**	**1024, 1536 and 2048 bits**
/TDESsession-DH	**DH Key Agreement Algorithm – 1024, 1536 and 2048 bits**	**112 bits**
/AESsession-DH	**DH Key Agreement Algorithm – 1024, 1536 and 2048 bits**	**128, 192, 256 bits**

Table 10: FCS_CKM.1/DH_PACE refinements

FCS_CKM.1/KeyPair Cryptographic key generation for Active Authentication

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or
FCS_COP.1]: fulfilled by **FCS_COP.1/AA**
FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note

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

iteration	algorithm	Key size	Standards
/RSA	**RSA CRT Key generation**	**1024, 1536 and 2048 bits**	**none (generation of random numbers and Miller- Rabin primality testing)**
/ECC	**ECC Key generation**	**160, 192, 224, 256, 320, 384, 512 and 521 bits**	***FIPS 186-3 Appendix B.4.1***

CA/DH	**DH key generation**	**1024, 1280, 1536 and 2048 bits**	ANSI X9.42

Table 11: FCS_CKM.1/KeyPair refinements

Application notes:

- The dependency of FCS_CKM1/KeyPair on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.
- In some configurations, Key pair generation is removed. FCS_CKM.1/KeyPair covers session key generation for secure channels opened in pre-personalization and personalization.

FCS_CKM.1/PERSO Cryptographic key generation – Symmetric session keys during pre-personalisation and personalisation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or FCS_COP.1]: fulfilled by **FCS_COP.1/PERSO**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**

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

iteration	algorithm	Key size	Standards
/TDES	**TDES ISK key derivation**	**112 bits**	**[ICAO-9303] normative appendix 5**
/GP	**GP session keys**	**112, 128 bits (and 192 & 256 bits for SCP03)**	**[GP211] SCP01, SCP02, or SCP03**

Table 12: FCS_CKM.1/PERSO refinements

Application note: FCS_CKM.1/Manuf covers session key generation for secure channels opened in pre-personalization and personalization.

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/PERSO**

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

Application note: Secure erasing of data is performed by overwriting the data with random numbers.

6.1.2.2 *Cryptographic operation (FCS_COP.1)*

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

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 in accordance with a specified cryptographic algorithm **Table 13 algorithm** and cryptographic key sizes **Table 13 Key size** that meet the following: **Table 13 list of standards**.

iteration	algorithm	Key size	List of standards
/ENC_TDES	**TDES in CBC mode**	**112 bits**	**ISO 10116**
/ENC_AES	**AES in CBC mode**	**128, 192, 256**	**ISO 10116**

Table 13: FCS_COP.1/PACE_ENC refinements

FCS_COP.1/PACE_MAC Cryptographic operation – MAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: 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 secure messaging – message authentication code in accordance with a specified cryptographic algorithm **Table 14 algorithm** and cryptographic key sizes **Table 14 Key size** that meet the following: compliant to [ICAO-TR-SAC].

iteration	algorithm	Key size	List of standards
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 14: FCS_COP.1/PACE_MAC refinements

FCS_COP.1/PERSO Cryptographic operation – Symmetric encryption, decryption, and MAC during pre-personalisation and personalisation

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/PERSO** FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.
FCS_COP.1.1 /PERSO	The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **Table 15 algorithm** and cryptographic key sizes **Table 15 key size** that meet the following: **Table 15 standards**.

iteration	algorithm	Key size	Standards
/ENC_TDES	**TDES encryption and decryption**	**112 bits**	**[SP 800-67]**
/ENC_AES	**AES encryption and decryption**	**128, 192, 256**	**[FIPS 197]**
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 15: FCS_COP.1/PERSO refinements

Application note: FCS_COP.1/PERSO covers encryption and decryption as well as MAC creation and verification for secure channels open in pre-personalization and personalization.

FCS_COP.1/AA Cryptographic operation – Active Authentication

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/KeyPair** FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note.
FCS_COP.1.1 /AA	The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **Table 16 algorithm** and cryptographic key sizes **Table 16 Key size** that meet the following: **Table 16 List of standards**.

iteration	algorithm	Key size	List of standards
/AA_RSA	**RSA**	**1024, 1280, 1536, 2048, 3072 and 4096 bits**	**ISO9796-2**

Table 16: FCS_COP.1/AA refinements

Application note:

- The dependency of FCS_COP.1/AA on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

6.1.2.3 Random Number Generation (FCS_RND.1)

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 **RGS [RGS-B1], and X931 with seed entropy at least 128 bits**.

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

6.1.3 Class FIA Identification and Authentication

For the sake of better readability, Table 17 provides an overview of the authentication mechanisms used:

Name	SFR for the TOE	Comments
Authentication protocol in pre-perso and perso phases	**FIA_UAU.1/PERSO** **FIA_AFL.1/PERSO**	as required by **FCS_CKM.1/PERSO**
PACE protocol	**FIA_UAU.1/PACE** **FIA_UAU.5/PACE** **FIA_AFL.1/PACE**	as required by **FCS_CKM.1/DH_PACE**
Passive Authentication	**FIA_UAU.5/PACE**	no related cryptographic operations by the TOE

Table 17: Overview of authentication SFR

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**
FIA_AFL.1.1 /PACE	The TSF shall detect when [**Number in Table 18**] 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 [**Actions in Table 18**].

Password	Number	Actions
MRZ, CAN	**1**	**Exponentially increase time delay before new authentication attempt is possible**.
PIN	**3**	**Block PIN**.

Table 18: FIA_AFL.1/PACE refinements

FIA_AFL.1/PERSO Authentication failure handling during pre-personalization and personalization phases

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by **FIA_UAU.1/PERSO**
FIA_AFL.1.1 /PERSO	The TSF shall detect when [**Number in Table 19**] unsuccessful authentication attempt occurs related to **authentication attempts using ISK key**.
FIA_AFL.1.2 /PERSO	When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**Actions in Table 19**].

Auth type	Number	Actions
GP	**3**	**Block GP authentication**.
ISK key	**3**	**Block ISK Key**.

Table 19: FIA_AFL.1/PERSO refinements

FIA_UID.1/PERSO Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 /PERSO	The TSF shall allow **1. to establish a communication channel,** **2. to carry out the mutual authentication Protocol according to [GP]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 /PERSO	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PERSO Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/PERSO**
FIA_UAU.1.1 /PERSO	The TSF shall allow **1. to establish a communication channel,** **2. to carry out the mutual authentication Protocol according to [GP]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 /PERSO	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

- FIA_AFL.1/PERSO, FIA_UID.1/PERSO, and FIA_UID.1/PERSO are extensions to [PP-MRTD-SAC], in order to deal with identification and authentication in pre-personalisation and personalisation phases.

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 a communication channel, 2. carrying out the PACE Protocol according to [TR-SAC] 3. to read the Initialization Data if it is not disabled by TSF according to **FMT_MTD.1/INI_DIS**. 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.

FIA_UAU.1/PACE Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/PACE**
FIA_UAU.1.1 /PACE	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE Protocol according to [TR-SAC] 3. to read the Initialization Data if it is not disabled by TSF according to **FMT_MTD.1/INI_DIS**, 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.

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1 /PACE	The TSF shall prevent reuse of authentication data related to 1.PACE Protocol according to [TR-SAC] 2.Authentication Mechanism based on **Triple-DES, AES**.

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.PACE Protocol according to [TR-SAC] , 2.Passive Authentication according to [ICAO-9303] 3.Secure messaging in MAC-ENC mode according to [TR-SAC] 4.Symmetric Authentication Mechanism based on **Triple-DES, AES** 5. Terminal Authentication according to [ICAO-9303] to support user authentication.
FIA_UAU.5.2 /PACE	The TSF shall authenticate any user's claimed identity according to the following rules: 1.Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol. 2.The TOE accepts the authentication attempt as Personalisation Agent by **the Symmetric Authentication Mechanism with Personalization Agent Key**.

Application note:

- Passive authentication and Active authentication are not user authentications, rather chip authentication. This ST includes them FIA_UAU.5/PACE to be consistent with [PP-MRTD-SAC].

FIA_UAU.6/PACE 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 each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[35]

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

Hierarchical to:	No other components
Dependencies:	No dependencies

FIA_API.1.1/AA	The TSF shall provide an **Active Authentication Protocol according to [ICAO-9303]** to prove the identity of the **TOE**.

Application note: This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generates a challenge then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corresponding to the Active Authentication public key (EF.DG15).

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

6.1.4 Class FDP User Data Protection

FDP_ACC.1/TRM Subset access control – Terminal Access

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by **FDP_ACF.1/TRM**
FDP_ACC.1.1 /TRM	The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data stored in the travel document and **None.**

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 initialisation: not fulfilled, but **justified** 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 Access Control SFP to objects based on the following: 1. Subjects: a. Terminal b. BIS-PACE 2. Objects: a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 , EF.SOD and EF.COM of the logical travel document, b. data in EF.DG3 of the logical travel document, c. data in EF.DG4 of the logical travel document, 3. Security attributes: a. authentication status of terminals
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: 1. A BIS-PACE is allowed to read data objects from **FDP_ACF.1/TRM** according to [ICAO-TR-SAC] after a successful PACE authentication as required by **FIA_UAU.1/PACE.**
FDP_ACF.1.3 /TRM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none .
FDP_ACF.1.4 /TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: 1. Any terminal being not authenticated as PACE authenticated BIS-PACE

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

FDP_RIP.1Subset 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** the following objects: 1. Session Keys (immediately after closing related communication session). 2. ephemeral private key ephem - SK_{PICC}- PACE (by having generated a DH shared secret *K*).

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 **FTP_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 to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM Data exchange integrity

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by **FTP_ITC.1/PACE** [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by **FDP_ACC.1/TRM**
FDP_UIT.1.1 /TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
FDP_UIT.1.2 /TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

6.1.5 Class FTP Trusted Path/Channels

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 ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

6.1.6 Class FAU Security Audit

FAU_SAS.1 Audit storage

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records.

6.1.7 Class FMT Security Management

The SFR FMT_SMF.1 and FMT_SMR.1/PACE provide basic requirements on the management of the TSF data.

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 management functions: 1.Initialization, 2.Pre-personalisation, 3.Personalisation, 4.Configuration.

FMT_SMR.1/PACE Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/PACE** and **FIA_UID.1/PERSO**.
FMT_SMR.1.1 /PACE	The TSF shall maintain the roles 1.Manufacturer , 2.Personalisation Agent, 3.Terminal, 4.PACE authenticated BIS-PACE
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

/PACE

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).

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

FMT_LIM.1 Limited capabilities

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by **FMT_LIM.2**
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 do not allow 1.User Data to be manipulated and disclosed, 2.TSF data to b e manipulated or disclosed, 3.software to be reconstructed, 4.substantial information about construction of TSF to be gathered which may enable other attacks.

FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by **FMT_LIM.1**.
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 do not allow 1.User Data to be manipulated and disclosed, 2.TSF data to be manipulated or disclosed, 3.software to be reconstructed, 4.substantial information about construction of TSF to be gathered which may enable other attacks

Application note: The term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation 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 the Initialisation Data and Pre-personalisation Data to the Manufacturer.

FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation 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 the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent

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

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 /KEY_READ	The TSF shall restrict the ability to read the 1. PACE passwords, 2. AA keys 3. Personalisation Agent Keys to none.

FMT_MTD.1/AAK 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/ AAK	The TSF shall restrict the ability to **create and load** the Active Authentication Private Key to **the Personalization Agent**.

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 the Document Security Object (SO_D) to the Personalisation Agent.

6.1.8 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for the 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)', 'Limited availability (FMT_LIM.2)' and 'Resistance to physical attack (FPT_PHP.3)' together with the design measures to be described within the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of the TOE security functionality.

FPT_EMS.1TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit **electromagnetic and current emissions** in excess of **intelligible threshold** enabling access to 1.PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 2.the ephemeral private key ephem - SK_{PICC}- PACE, 3.**EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG16**.
FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface travel document's contactless/contact interface and circuit contacts to gain access to 1.PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 2.the ephemeral private key ephem - SK_{PICC}- PACE, 3.**EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG6 to EF.DG16**.

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

FPT_FLS.1Failure 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**,

FPT_TST.1TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests **Conditions under which self test should occur** to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity

of stored TSF executable code.

Conditions under which self test should occur	Description of the self test
During initial start-up	**RNG live test, sensor test, FA detection, Integrity Check of NVM ES**
Periodically	**RNG monitoring, FA detection**
After cryptographic computation	**FA detection**
Before any use or update of TSF data	**FA detection, Integrity Check of related TSF data**

Table 20: FPT_TST refinements

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL5 augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 Security Functional Requirements Rationale

This rationale is based on [PP-MRTD-SAC] §6.3.1.

The following table provides an overview for security functional requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

	OT.Identification	OT.AC_Pers	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_Malfuntion	OT.Activ_Auth_Proof
FCS_CKM.1/DH_PACE			X	X	X						
FCS_CKM.1/PERSO			X		X						
FCS_CKM.1/KeyPair											X
FCS_CKM.4			X	X	X						
FCS_COP.1/PACE_ENC					X						
FCS_COP.1/PACE_MAC			X	X							

FCS_COP.1/AA											X
FCS_COP.1/PERSO			X		X						
FCS_RND.1			X	X	X						
FIA_AFL.1/PERSO			X		X						
FIA_AFL.1/PACE						X					
FIA_UID.1/PACE			X	X	X						
FIA_UID.1/PERSO		X	X		X						
FIA_UAU.1/PACE			X	X	X						
FIA_UAU.1/PERSO		X	X		X						
FIA_UAU.4/PACE			X	X	X						
FIA_UAU.5/PACE			X	X	X						
FIA_UAU.6/PACE			X	X	X						
FIA_API.1/AA											X
FDP_ACC.1/TRM			X		X						
FDP_ACF.1/TRM			X		X						
FDP_RIP.1			X	X	X						
FDP_UCT.1/TRM			X		X						
FDP_UIT.1/TRM			X		X						
FTP_ITC.1/PACE			X	X	X	X					
FAU_SAS.1	X	X									
FMT_SMF.1	X	X	X	X	X						
FMT_SMR.1/PACE	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/KEY_READ		X	X	X	X						X
FMT_MTD.1/AAK											X
FMT_MTD.1/PA		X	X	X	X						
FPT_EMS.1								X			
FPT_FLS.1								X		X	
FPT_TST.1								X		X	
FPT_PHP.3			X					X	X		

Table 21: Coverage of Security Objectives for the TOE by SFR

A detailed justification required for *suitability* of the security functional requirements to achieve the security objectives is given below.

The security objective **OT.Identification** 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** aims that only Personalisation Agent can write the User- and the TSF-data into the TOE.
The justification for the SFR **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.

FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalisation data).
The SFR **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related. The SFR **FMT_MTD.1/KEY_READ** restricts the access to the Personalisation Agent Keys.
The SFR **FIA_UID.1/PERSO** and **FIA_UAU.1/PERSO** ensure the authentication of the agent in pre-personalization and personalization phases.

The security objective **OT.Data_Integrity** aims that the TOE always ensures integrity of the User- and TSF-data stored and, after the PACE authentication, of these data exchanged (physical manipulation and unauthorised modifying).
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**).
FIA_UAU.4/PACE, **FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the protocols used.
Unauthorised modifying of the exchanged data is addressed, in the first line, by **FDP_UCT.1/TRM**, **FDP_UIT.1/TRM** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_MAC**. 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**. **FDP_RIP.1** requires erasing the values of session keys (here: for K_{MAC}). The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords.
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 SFR **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.
In pre-personalization and personalization phases, **FCS_COP.1/PERSO**, supported by **FCS_CKM.1/PERSO**, ensure the integrity and confidentiality of data transfers; **FIA_UID.1/PERSO**? **FIA_AFL.1/PERSO**and **FIA_UAU.1/PERSO** ensure the authentication of the agent.

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 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**. **FDP_RIP.1** requires erasing the values of session keys (here: for K_{MAC}). The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords.
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.
FIA_UAU.4/PACE, **FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the protocols used.
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_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE 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**. 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**. **FDP_RIP.1** requires erasing the values of session keys (here: for Kenc). The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords.
FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization 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.
In pre-personalization and personalization phases, **FCS_COP.1/PERSO**, supported by **FCS_CKM.1/PERSO**, ensure the integrity and confidentiality of data transfers; **FIA_UID.1/PERSO**, **FIA_AFL.1/PERSO** and **FIA_UAU.1/PERSO** ensure the authentication of the agent.

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/contact interface of the TOE without a priori knowledge of the correct values of shared PACE passwords. This objective is achieved as follows:
(i) while establishing PACE communication with a PACE password (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_Abuse_Func** aims preventing TOE's functions being not intended to be used in the operational phase from manipulating and disclosing the User- and TSF-data.This objective is achieved by **FMT_LIM.1** and **FMT_LIM.2** preventing misuse of test and other functionality of the TOE having not to be used in the TOE's operational life cycle phase.

The security objective **OT.Prot_Inf_Leak** aims protection against disclosure of confidential User- or/and TSF-data stored on / processed by the TOE. This objective is achieved
- by **FPT_EMS.1** for measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
- by **FPT_FLS.1** and **FPT_TST.1** for forcing a malfunction of the TOE, and
- by **FPT_PHP.3** for a physical manipulation of the TOE.

The security objective **OT.Prot_Phys-Tamper** aims protection of the confidentiality and integrity of the User- and TSF-data as well as embedded software stored in the TOE.
This objective is completely covered by **FPT_PHP.3** in an obvious way.

The security objective **OT.Prot_Malfunction** aims ensuring a correct operation of the TOE by preventing its operation outside the normal operating conditions.
This objective is covered by **FPT_TST.1** requiring self tests to demonstrate the correct operation of the TOE and tests of authorised users to verify the integrity of the TSF-data and the embedded software (TSF code) as well as by **FPT_FLS.1** requiring entering a secure state of the TOE in case of detected failure or operating conditions possibly causing a malfunction.

The security objective OT.Activ_Auth_Proof aims at proving the authenticity of the TOE.
This objective is mainly covered by **FIA_API.1/AA**. It is supported **FCS_COP.1/AA** which covers the authentication algorithm and by **FCS_CKM.1/KeyPair** which covers the on-board generation of the authentication key. It is supported by **FMT_MTD.1/AAK** which controls the import and the generation of the authentication key. This objective is also supported by **FMT_MTD.1/KEY_READ** which protects the authentication key.

6.3.2 Rationale for SFR's Dependencies

The rationale in this paragraph is based on the rationale of [PP-MRTD-SAC] §6.3.2.

SFR	Dependencies	Support of the dependencies
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	**FCS_COP.1/PACE_ENC** & **FCS_COP.1/PACE_MAC** **FCS_CKM.4**
FCS_CKM.1/KeyPair	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	**FCS_COP.1/AA** **FCS_CKM.4**
FCS_CKM.1/PERSO	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	**FCS_COP.1/PERSO** **FCS_CKM.4**
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	**FCS_CKM.1/DH_PACE** & **FCS_COP.1/PERSO**
FCS_COP.1/PACE_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**FCS_CKM.1/DH_PACE** **FCS_CKM.4**
FCS_COP.1/PACE_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**FCS_CKM.1/DH_PACE** **FCS_CKM.4**
FCS_COP.1/PERSO	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**FCS_CKM.1/PERSO** **FCS_CKM.4**
FCS_COP.1/AA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	**FCS_CKM.1/KeyPair** Not fulfilled: see note 1
FCS_RND.1	No dependencies	none
FIA_AFL.1/PACE	FIA_UAU.1	**FIA_UAU.1/PACE**
FIA_AFL.1/PERSO	FIA_UAU.1	**FIA_UAU.1/PERSO**
FIA_UID.1/PACE	No dependencies	none
FIA_UAU.1/PACE	FIA_UID.1	**FIA_UID.1/PACE**
FIA_UAU.4/PACE	No dependencies	none
FIA_UAU.5/PACE	No dependencies	none
FIA_UAU.6/PACE	No dependencies	none
FIA_UID.1/PERSO	No dependencies	none
FIA_UAU.1/PERSO	FIA_UID.1	**FIA_UID.1/PERSO**
FIA_API.1/AA	No dependencies	none
FDP_ACC.1/TRM	FDP_ACF.1	**FDP_ACF.1/TRM**
FDP_ACF.1/TRM	FDP_ACC.1 FMT_MSA.3	**FDP_ACC.1/TRM** Not fulfilled: see note 2
FDP_RIP.1	No dependencies	none

SFR	Dependencies	Support of the dependencies
FDP_UCT.1/TRM	[FTP_ITC.1, or FTP_TRP.1] [FDP_ACC.1, or FDP_IFC.1]	**FTP_ITC.1/PACE** **FDP_ACC.1/TRM**
FDP_UIT.1/TRM	[FTP_ITC.1, or FTP_TRP.1] [FDP_ACC.1, or FDP_IFC.1]	**FTP_ITC.1/PACE** **FDP_ACC.1/TRM**
FTP_ITC.1/PACE	No dependencies	none
FAU_SAS.1	No dependencies	none
FMT_SMF.1	No dependencies	none
FMT_SMR.1/PACE	FIA_UID.1	**FIA_UID.1/PACE** **FIA_UID.1/PERSO**.
FMT_LIM.1	FMT_LIM.2	**FMT_LIM.2**
FMT_LIM.2	FMT_LIM.1	**FMT_LIM.1**
FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1** **FMT_SMR.1/PACE**
FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1** **FMT_SMR.1/PACE**
FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1** **FMT_SMR.1/PACE**
FMT_MTD.1/AAK	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1** **FMT_SMR.1/PACE**
FMT_MTD.1/PA	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1** **FMT_SMR.1/PACE**
FPT_EMS.1	No dependencies	none
FPT_FLS.1	No dependencies	none
FPT_TST.1	No dependencies	none
FPT_PHP.3	No dependencies	none

Table 22: SFR dependencies rationale

Notes:

1. The dependency between **FCS_COP.1/AA** and **FCS_CKM.4** is not fulfilled because the key is permanently stored on the card.
2. 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.

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance package EAL5. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL5 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional 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 sensitive material.

The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 3, entry 'Attacker'). This decision represents a part of the conscious security policy for the travel document required by the travel document Issuer and reflected by the current PP.

The set of *assurance* requirements being part of EAL5 fulfils all dependencies a priori.

The augmentation of EAL5 chosen comprises the following assurance components:

- ALC_DVS.2 and
- AVA_VAN.5.

For these additional assurance components, all dependencies are met or exceeded in the EAL5 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL5)		
ALC_DVS.2	no dependencies	-
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.5
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

Table 23: SAR Dependencies

6.3.4 Security Requirements – Internal Consistency

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

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

The dependency analysis in section 6.3.2 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in sec. 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 package EAL5 is a pre-defined set of 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 internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.2 Rationale for SFR's Dependencies 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, there are no inconsistencies between the goals of these two groups of security requirements.

6.3.5 Compatibility between SFR of [ST-SAC] and [ST-IC]

FAU_SAS.1 of [ST-SAC] is included in FAU_SAS.1 of [ST-IC].
FCS_RND.1, FCS_CKM.1 and FCS_COP.1 of [ST-SAC] are supported by FCS_CKM.1, FCS_COP.1 of [ST-IC].
FPT_EMS.1 and FPT_PHP.3 of [ST-SAC] are included in FPT_PHP.3 of [ST-IC].
FPT_FLS.1 of [ST-SAC] is included in FPT_FLS.1 of [ST-IC].

FCS_CKM.4, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_AFL.1, FIA_API, FDP_ACC.1, FDP_ACF.1, FDP_RIP.1, FDP_UCT.1, FDP_UIT.1, FTP_ITC.1, FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1, and FPT_TST.1 are specific to [ST-SAC] and they do not conflict with [ST-IC].

We can therefore conclude that the SFR of [ST-SAC] and [ST-IC] are consistent.

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the MultiApp v3 embedded software (including the optional NVM ES) and by the chip.

7.1.1 TSFs provided by the MultiApp v3 Software

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.AA	Active Authentication

Table 24: Security Functions provided by the MultiApp v3 Software

The SF.REL function provides the protection of data on the TOE. It encompasses:

- physical protection of the TOE as defined in **FPT_PHP.3**, **FPT_EMS.1**, **FPT_FLS.1**,
- the test mechanisms as defined in **FPT_TST.1**,
- protection against misuse of tests as defined in **FMT_LIM.1** and **FMT_LIM.2**.

The SF.AC function provides the access control of the TOE. It encompasses:

- the access control by the terminal as defined in **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM**,
- the access control to specific data as defined in **FAU_SAS.1**, **FMT_MTD.1/INI_ENA**, **FMT_MTD.1/INI_DIS**, **FMT_MTD.1/KEY_READ**, **FMT_MTD.1/AAK**, and **FMT_MTD.1/PA**,
- the role management as defined in **FMT_SMR.1/PACE**,
- the management functions linked to the different states of the TOE as defined in **FMT_SMF.1**.

The SF.SYM_AUTH function provides the symmetric authentication functions to the TOE. It encompasses:

- the PACE identification and authentication as defined in **FIA_AFL.1/PACE**, **FIA_UID.1/PACE**, **FIA_UAU.1/PACE**, **FIA_UAU.4/PACE**, **FIA_UAU.5/PACE**, and **FIA_UAU.6/PACE**,
- the identification and authentication in personalisation phase as defined in **FIA_AFL.1/PERSO**, **FIA_UID.1/PERSO**, and **FIA_UAU.1/PERSO**,
- The role authentication as requested by **FMT_SMR.1/PACE.**

The SF.SM function provides the secure massaging of the TOE. It encompasses:

- the establishment of SM as defined in **FTP_ITC.1/PACE**,
- the secure transfer of data through SM as defined in **FDP_UCT.1/TRM** and **FDP_UIT.1/TRM**,
- the cryptographic mechanisms used for the authentication and the SM, as defined in **FCS_CKM.1/DH_PACE**, **FCS_COP.1/PACE_ENC**, **FCS_COP.1/PACE_MAC**, **FCS_COP.1/PERSO**, and **FCS_RND.1**. Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function.
- the erasure of session keys as defined in **FCS_CKM.4** and **FDP_RIP.1**.

The SF.AA function provides the active authentication. It encompasses:

- the AA protocol itself as defined in **FIA_API.1/AA**,
- the AA cryptographic algorithm as defined in **FCS_COP.1/AA**,

- the generation and input of AA keys, as defined in **FCS_CKM.1/KeyPair** and **FMT_MTD.1/AAK**.

7.1.2 TSF provided by the M7820 chip

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC]. The IC and its primary embedded software have been evaluated at level EAL 5+.

SF	Description
SF_DPM	Device phase management
SF_PS	Protection against snooping
SF_PMA	Protection against modifying attacks
SF_PLA	Protection against logical attacks
SF_CS	Cryptographic support

Table 25: Security Functions provided by the M7820 chip

These SF are described in [ST-IC].

8. GLOSSARY AND ACRONYMS

Glossary

Term	Definition
Active Authentication	Security mechanism defined in [PKI] 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 of organization.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Application note	Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer
Basic Access Control (BAC)	Security mechanism defined in [PKI] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[36] and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (travel document details data and biographical data) stored on the travel document. See also par. 1.2.5; also [PKI].
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority[37] and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. A technical system being used by an inspecting authority and verifying the ePass presenter as the ePass holder (for ePassport: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass holder). The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol.
Biographical data (biodata)	The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).
Card Access Number	A short password that is printed or displayed on the document. The CAN is a

[36] an inspecting authority; concretely, by a control officer
[37] concretely, by a control officer

Term	Definition
(CAN)	non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [ICAO-TR-SAC]
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means [PKI].
Country Signing CertA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePasss and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [PKI], 5.5.1.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data transmitted between the TOE and an inspection system using BAC [PKI]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [PKI].
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SOD)	A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the ePassport application (EF.SOD) of the travel document. It may carry the Document Signer Certificate (CDS); see [PKI], sec. A.10.4.
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS)(CDS), see [PKI]. This role is usually delegated to a Personalisation Agent.
Eavesdropper	A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document.
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; see [PKI].
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [ICAO-TR-SAC].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [PKI].
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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [PKI].
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures

Term	Definition
	between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
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; see [PKI].
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [PKI].
Initialisation Data	Any data defined by the travel document manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as travel document material (IC identification data).
Inspection	The act of an official organisation (inspection authority) examining an travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [PKI].
Inspection system	see BIS-PACE for this PP. see also BIS-BAC for general information
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements stored upon have not been altered from that created by the travel document Issuer.
Issuing Organisation	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [PKI].
Issuing State	The country issuing the travel document; see [PKI].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [PKI]. The capacity expansion technology used is the travel document's chip.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods; see [PKI]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
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; see [PKI].
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life-cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ).
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the

Term	Definition
	Card/Chip or Document Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [PKI].
Passport (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO-TR-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document.
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i)establishing the identity of the travel document holder for the biographic data in the travel document, (ii)enrolling the biometric reference data of the travel document holder, (iii)writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data,) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase card issuing.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.
Receiving State	The Country to which the travel document holder is applying for entry; see [PKI].
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443]

Term	Definition
Rightful equipment (rightful terminal or rightful Card)	A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see Inspection System).
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [PKI].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Skimming	Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-SAC], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.
Supplemental Access Control	A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.
Terminal	A Terminal is any technical system communicating with the TOE through a contactless / contact interface.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [PKI] (there "Machine readable travel document").
Travel document (electronic)	The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
Travel document holder	A person for whom the ePass Issuer has personalised the travel document.
Travel document Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the travel document holder
Travel document presenter	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalised travel document	travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip.
User Data	All data (being not authentication data) (i)stored in the context of the ePassport application of the travel document as defined in [PKI]and (ii)being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
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

Term	Definition
	reference data known for the claimed identity.

Acronyms

Acronym	Term
AA	Active Authentication
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [9])
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RF	Radio Frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [ICAO-TR-SAC]
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)