IDEMIA

LDS V10.1 Applet in PACE Configuration with CAM

Public Security Target

About IDEMIA

OT-Morpho is now IDEMIA, the global leader in trusted identities for an increasingly digital world, with the ambition to empower citizens and consumers alike to interact, pay, connect, travel and vote in ways that are now possible in a connected environment.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, we reinvent the way we think, produce, use and protect this asset, whether for individuals or for objects. We ensure privacy and trust as well as guarantee secure, authenticated and verifiable transactions for international clients from Financial, Telecom, Identity, Security and IoT sectors.

With close to €3bn in revenues, IDEMIA is the result of the merger between OT (Oberthur Technologies) and Safran Identity & Security (Morpho). This new company counts 14,000 employees of more than 80 nationalities and serves clients in 180 countries.

| For more information, visit www.idemia.com / Follow @IdemiaGroup on Twitter

DOCUMENT MANAGEMENT

Business Unit – Department	**CI – R&D**
Document type	**FQR**
Document Title	**LDS V10.1 Applet in PACE Configuration with CAM – Public Security Target**
FQR No	**550 0078**
FQR Issue	**4**

DOCUMENT REVISION

Date	Revision	Modification
2020/02/25	1	Creation of the document
2020/03/06	2	Updated IC reference
2020/04/21	3	Added updated platform certificate
2020/06/03	4	Updated after incorporating ANSSI feedback

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Security Target introduction

This Security Target aims to satisfy the requirements of Common Criteria level EAL5+, augmented with AVA_VAN.5 and ALC_DVS.2 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.
The basis for this composite evaluation is the composite evaluation of open platform *COSMO V8.2* and configurable Java Card application, LDS V10.1.

The LDS V10.1 can have different configurations as described in Section 2.1. The present ST considers configuration 1 defined in Table 5 that supports the following features:

- PACE
- AA
- CA
- CAM

It is activated in ROM during pre-personalization phase.
The LDS works on the ID-One Cosmo v8.2 Platform. The platform is covered by the Security Target [54].

1.1 Security target Reference

This Security target is identified as follows:

Title	LDS V10.1 Applet in PACE Configuration with CAM – Public Security Target
ST Identification	FQR 550 0078 Ed 4
CC Version	3.1 Revision 5
Assurance Level	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
ITSEF	CEA-LETI
Certification Body	ANSSI
Compliant To Protection Profile	PP- PACE [50]

Table 1: ST Reference

1.2 TOE References

TOE Commercial Name	LDS V10.1 in PACE configuration with CAM on ID-One Cosmo V8.2
Applet Code Version	06 70 01 2F
Platform Codop Identification	09 47 41
Guidance Documents	[60], [61], [55], [56], [57] and [58]
Platform Name	ID-One Cosmo v8.2 Platform
Platform Certificate	ANSSI-CC-2020/26
Communication Protocol	Contact, Contactless and Dual
IC Identifier	NXP Secure Smart Card Controller P6022Y VB
IC Certificate	BSI-DSZ-CC-1059-V3-2019 BSI-DSZ-CC-1059-2018

Table 2: TOE References

Note: For the LDS applet to function in the certified configuration, the patch code identified in the table above needs to be present in the platform. Its presence can be checked as described in Section 3.1 of [60] or Section 2.2 of [61].

1.3 TOE Identification

The aim of the paragraphs is to allow the user to identify uniquely the TOE.

The TOE is composed of application [LDS V10.1 in PACE configuration with CAM] and COSMO v8.2 Platform on the IC.

1.3.1 TOE Identification

This chapter presents the means to identify the evaluated application and the Platform.

The **[**LDS V10.1 Security Target PACE**]** installation command **shall** use the executable load File AID and module AID:

Name	Value
Executable Load File (ELF) AID	A000000077010000071000000000005
Executable Module AID	A000000077010000071000010000005
Application AID	A00000024710FF

Table 3: AID LDS V10.1 Security Target PACE Application

1.3.2 Platform Identification

In order to assure the authenticity of the card, the product identification shall be verified by analysing:

Platform Name	**ID-One Cosmo v8.2 Platform**
Mask / Hardware Identification	091121
Label GIT code	IDOne_Cosmo_V8.2_091121
IC reference version	NXP P60D145
IC configuration	NXP P6022y VB
IC ST identification	1. NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 2.6 — 23 August 2019 BSI-DSZ-CC-1059-V3-2019 2. NXP Secure Smart Card Controller P6022y VB Security Target Lite Rev. 2.1 - 6 April 2018 BSI-DSZ-CC-1059-2018
IC EAL	EAL6 with augmentations: ALC_FLR.1 and ASE_TSS.2
IC certificate	BSI-DSZ-CC-1059-V3-2019 BSI-DSZ-CC-1059-2018

Table 4: Platform Identification

1.3.3 Configuration of the platform

In the present evaluation, the loading of application (Java Card Applets) on the platform at use phase is allowed. It can be forbidden if requested by the product issuer.

1.4 References

[1] Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", April 2017, Version 3.1 revision 5.
[2] Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", April 2017, Version 3.1 revision 5.
[3] Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", April 2017, Version 3.1 revision 5.
[4] Composite product evaluation for Smart Cards and similar devices", April 2012, Version 1.2, CCDB-2012-04-001.
[5] JIL - Certification of "open" smart card products - Version 1.1 - 4 February 2013
[6] Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices Version 1.5.1, May 2018
[7] Global Platform Card Specification – Version 2.2.1 – January 2011.
[8] Global Platform Card Mapping Guidelines of existing GP v2.1.1 implementations on v2.2.1 – Version 1.0.1 – January 2011.
[9] Global Platform Card Technology, Security Upgrade for Card Content Management, Card Specification v 2.2 – Amendment E – Version 0.14 – October 2011.
[10] Global Platform Card Technology, Secure Channel Protocol 03, Card - Specification v 2.2 - Amendment D- Version 1.1 - September 2009.
[11] Identification cards - Integrated Circuit(s) Cards with contacts, Part 6: Inter industry data elements for interchange", ISO / IEC 7816-6 (2004).
[12] FIPS PUB 46-3 "Data Encryption Standard", October 25, 1999, National Institute of Standards and Technology
[13] FIPS PUB 81 "DES Modes of Operation", December, 1980, National Institute of Standards and Technology
[14] FIPS PUB 140-2 "Security requirements for cryptographic modules", May 2001, National Institute of Standards and Technology
[15] FIPS PUB 180-3 "Secure Hash Standard", October 2008 , National Institute of Standards and Technology
[16] FIPS PUB 186-3 "Digital Signature Standard (DSS)", June 2009, National Institute of Standards and Technology
[17] FIPS PUB 197, "The Advanced Encryption Standard (AES)", November 26, 2001, National Institute of Standards and Technology
[18] SP800_90 "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", March 2007, National Institute of Standards and Technology
[19] NIST Special Publication 800-38B, Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005
[20] CEN/EN14890:2013 Application Interface for smart cards used as Secure Signature Creation
[21] ANSI X9.31 "Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)", 1998, American National Standards Institute
[22] ISO/IEC 9796-1, Public Key Cryptography using RSA for the financial services industry", annex A, section A.4 and A.5, and annex C (1995)
[23] ISO/IEC 9797-1, "Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher", 1999, International Organization for Standardization
[24] ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function
[25] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002
[26] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[27] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002
[28] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993
[29] FIPS 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
[30] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 September 1998
[31] PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993
[32] IEEE Std 1363a-2004, "Standard Specification of Public Key Cryptography – Amendment 1: Additional techniques", 2004, IEEE Computer Society.
[33] Référentiel Général de Sécurité version 2.0 – Annexe B1 – Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014
[34] AIS 31 - Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik
[35] European Card for e-Services and national e-ID Applications - IAS ECC v1.0.1
[36] ISO/IEC 7816-4:2013, Identification Cards — Integrated circuit cards— Part 4 : Organization, security and commands for interchange
[37] ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
[38] ISO 11568-2:2012, Financial services - Key management (retail) - Part 2 : symmetric ciphers, their key management and life cycle
[39] Technical Guideline TR-03111- Elliptic Curve Cryptography Version 2.0
[40] Référentiel général de sécurité, version 2.0 du 21 février 2014 - Annexe B1 - Mécanismes cryptographiques
[41] ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996
[42] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization
[43] 'ICAO Doc 9303', Machine Readable Travel Documents, Seventh Edition, 2015 – Security Mechanisms for MRTDs
[44] Development of a logical data structure – LDS for optional capacity expansion technologies Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18
[45] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v2.20
[46] Annex to Section III Security Standards for Machine Readable Travel Documents Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003
[47] BAC- Machine readable travel documents with "ICAO Application", Basic Access control – BSI-PP-0055 v1.10 25th march 2009
[48] EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
[49] EAC With PACE- Machine readable travel documents with "ICAO Application", Extended Access Control with PACE (EAC PP) – BSI-PP-0056 V2 – 2012
[50] Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) – BSI-CC-PP-0068-V2-2011-MA-01

[51] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007
[52] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009
[53] Technical Report, Supplemental Access Control for Machine Readable Travel Documents – version v1.01
[54] FQR 110 9067 Ed 8.0 – ID-ONE COSMO v8.2 – Public Security Target
[55] ID-One Cosmo V8.1-n, Application Loading Protection Guidance, FQR: 110 8001, Issue 1
[56] ID-One Cosmo V8.2, Security Recommendations, FQR: 110 8963, Ed 4
[57] ID-One Cosmo V8.2, Pre-Perso Guide, FQR: 110 8875, Ed 9
[58] ID-One Cosmo V8.2, Reference Guide, FQR 110 8885, Ed 8
[59] LDS EAC JAVA Applet SOFTWARE REQUIREMENTS SPECIFICATIONS –0670012 00 SRS AA
[60] FQR 220 1424 Ed5 – AGD_PRE
[61] FQR 220 1425 Ed3 – AGD_OPE

2 Target of Evaluation

The product **LDS V10.1** is a multi-applicative Java Card product, embeddable in contact and/or contact-less smart card integrated circuits of different form factors. The product can be configured to serve different use cases, during the **Pre-Personalization/Personalization phases** of the product [60].

The product supports the storage and retrieval of structured information compliant to the Logical Data Structure as specified in [44]. It also provides standard authentication protocols, PACE [50], Chip Authentication and Active Authentication.

It can host two types of applications as mentioned above, namely the **IDL** and **MRTD**. Moreover, further configuration may also be done to each type of application to serve use cases other than those behaviourally defined in the referenced normative documents.

This product is loaded on the platform, for details see ST [54].
The LDS V10.1 product architecture can be viewed as shown in the following figure:

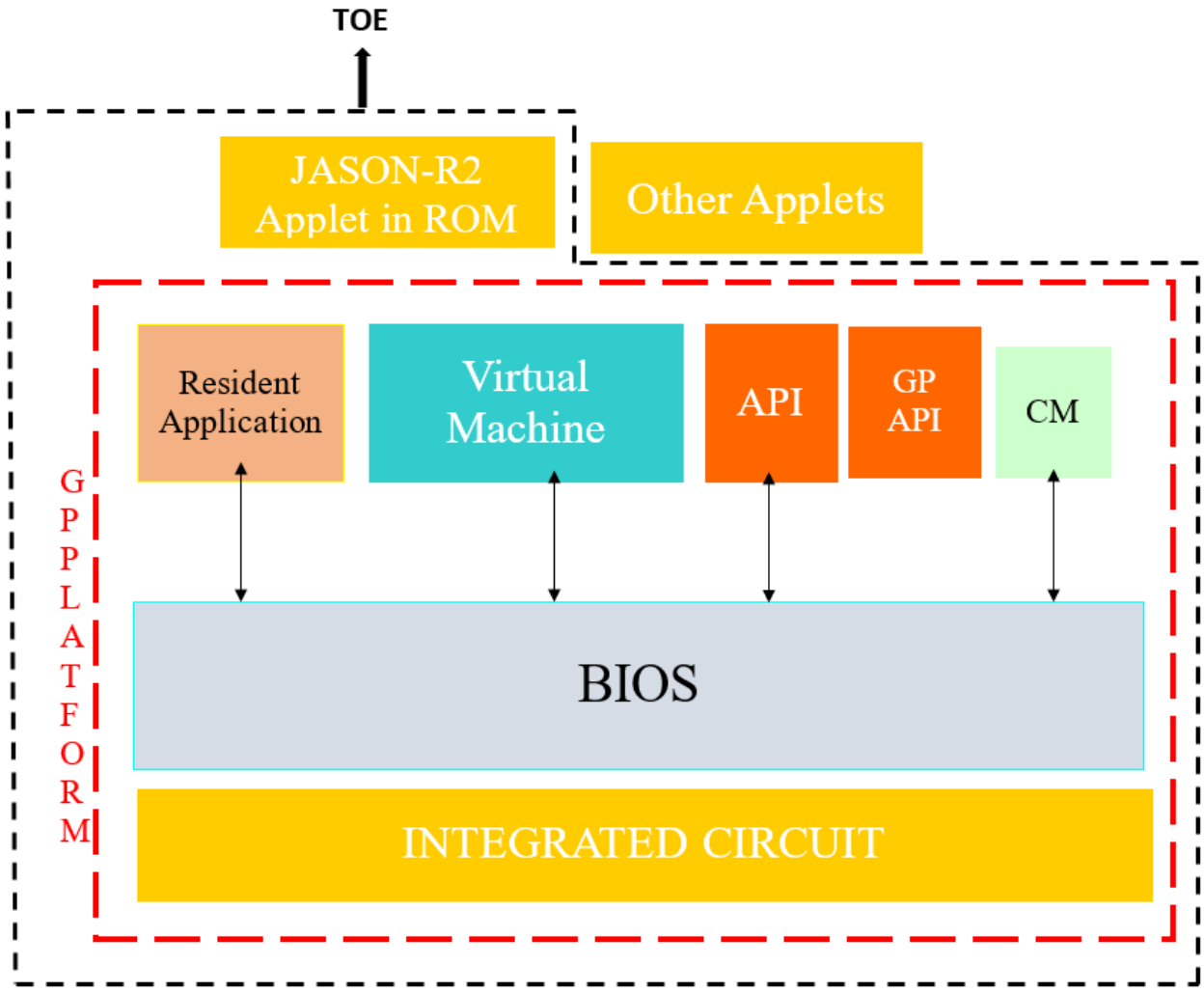

Figure 1: LDS V10.1 on Cosmo V8.2 Overview

2.1 TOE overview

The TOE described in this security target is the PACE, conformant to Configuration 1 (below). The product is composed of the functions: AA, CAM, PACE and CA which are all presented in the chapter TOE architecture. Only some parts are in the scope of the evaluation of the present configuration.

Different configurations of the TOE are under evaluation. This ST considers only PACE, CA, AA and CAM.

Configuration	PP Conformity	Extensions
1	**PP 0068 (PACE)**	**AA** **CA** **CAM**
2	PP0056v2 (EAC with PACE)	AA CAM PACE-CAM/TA without CA BAC de-activation SM (DES + AES) on read DG3+DG4 After EAC
3	PP 0055 (BAC)	AA + CA
4	PP0056v1 (EAC with BAC)	AA SM (DES + AES) on read DG3+DG4 after EAC

Table 5: 4 Configurations of the LDS application

The PACE TOE is instantiated during the application Pre-personalization with the creation of the MF / DF required for this configuration.

In the use phase of the product, and for interoperability purposes, the MRTD will most likely support BAC, PACE and EAC.

- If the terminal reads the content of the MRTD by performing BAC then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance [54] and the TOE described by the ST claiming compliance to PP EAC assuming PACE is not supported (as not used for the inspection procedure).
- If the terminal reads the content of the MRTD by performing PACE then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance to PP with PACE assuming BAC is not supported (as not used for the inspection procedure).

The TOE life cycle is described in **§ 3.**
The TOE identification is described in **§ 1.3.1.**

The TOE scope encompasses the following features:

- Active Authentication
- PACE_CAM Authentication
- Chip Authentication

Nevertheless, the TOE in the LDS application embeds other secure functionalities they are not in the scope of this evaluation and are in the scope of other evaluations.

2.1.1 Physical Scope

The TOE is physically made up of several components hardware and software. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the

microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.
The TOE may be used on several physical medium within an inlay, or eCover; in a plastic card.

The physical form of the module is depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure.

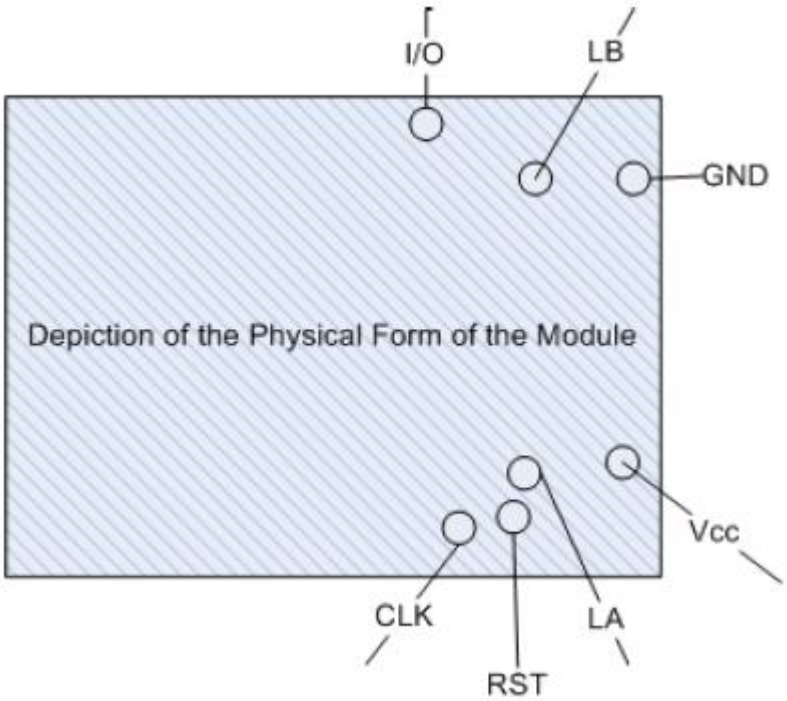

Figure 2: Physical Form

The contactless ports of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers and antenna connections as input/output devices.

Port	Description	Logical Interface Type
VCC, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816:Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/ Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 6: Ports and Interfaces

2.1.2 Required non-TOE hardware/software/firmware

The TOE is an MRTD. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate the TOE needs a card reader.

2.1.3 TOE Usage and major security features

State or organisation issues MRTDs to be used by the holder to prove his/her identity and claiming associated rights. For instance, it can be used to check identity at customs in an MRTD configuration, verifying authenticity of electronic visa stored on the card and correspondence with the holder.

In order to pass successfully the control, the holder presents its personal MRTD to the inspection system to first prove his/her identity. The inspection system is under control of an authorized agent and can be either a desktop device such as those present in airports or a portable device to be used on the field.

The MRTD in context of this security target contains:

- Visual (eye readable) biographical data and portrait of the holder printed in the booklet
- A separate data summary (MRZ or keydoc data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ or keydoc area)
- And data elements stored on the TOE's chip for contact-less machine reading.

The authentication of the holder is based on:

- The possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and
- The Biometric matching performed on the Inspection system using the reference data stored in the MRTD.

When holder has been authenticated the issuing State or Organization can perform extra authentications in order to gain rights required to grant access to some sensitive information such as "visa information".

The issuing State or Organization ensures the authenticity of the data of genuine MRTDs. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The MRTD can be viewed as the combination:

A physical MRTD in form of paper or plastic with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to)

- personal data of the MRTD holder
- The biographical data on the biographical data page of the passport book
- The printed data in the Machine-Readable Zone (MRZ) or keydoc area that identifies the device
- The printed portrait

A logical MRTD as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO and extended in [44][45][46] on the contactless integrated circuit. It presents contact or contact-less readable data including (but not limited to)

- personal data of the MRTD holder
- The digital Machine Readable Zone Data (digital MRZ data or keydoc data, DG1)
- The digitized portraits
- The optional biometric reference data of finger(s) or iris image(s) or both
- The other data according to LDS (up to DG24)
- The Document security object

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The MRTD as the physical device and the MRTD's chip is uniquely identified by the document number.
The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organisational security measures (e.g. control of materials, personalization procedures). These security measures include the binding of the MRTD's chip to the physical support.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional

security measure in the ICAO Doc 9303, and Password Authenticated Connection Establishment. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.
The Security Target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the PACE. This protection profile addresses the Chip Authentication Version 1 and Active Authentication.

The Active Authentication authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC. For this purpose the contactless IC contains its own Active Authentication Key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (Public Key (KPuAA) info) is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPrAA) is stored in the contactless IC's secure memory. By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SOD)) in combination with the challenge response, using the eMRTD's Active Authentication Key Pair (KPrAA and KPuAA), the inspection system verifies that the Document Security Object (SOD) has been read from the genuine contactless IC, stored in the genuine eMRTD.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE considers high attack potential.
For the PACE protocol, the following steps shall be performed:

(i) The travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging).
The Chip Authentication defined in [TR_03110] is a security feature which is optionally supported by the TOE. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

2.2 TOE Definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing and provides standard authentication protocols, namely PACE, Chip Authentication and Active Authentication.
The product can be configured to serve different use cases, during the **Pre-Personalization/personalization phases** of the product.
The TOE comprises at least:

Circuitry of the MRTD's chip (the integrated circuit, IC)

IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
Cosmo V8.2 Platform
API
LDS V10.1 application
Associated guidance documentation

The platform provides an operational environment for the application: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by the platform. The code for this functionality is contained in the platform ROM. However, the factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of Global Platform services),
The applet may be used on a contact mode compliant to ISO/IEC 7816-3 specification or on contactless mode compliant to ISO/IEC 14443 specification.

2.3 TOE Architecture

The TOE is a smartcard, composed of various modules and composed of the following components:

2.3.1 Integrated Circuit

The TOE is embedded on NXP chips; more information on the chips is given in the related Public Security Target identified in table 3 of chapter 1.3.2**.**

2.3.2 Java Card Platform

The Operating System is based on Java Card Technology and Global Platform technology. His main responsibilities are:

- providing interface between the Integrated Circuit and the applet
- providing to the applet, basic services to access to memories and all needed cryptographic operations
- ensuring global management of the card (loading, installation and deletion of applets) and monitor the security of the card (data integrity and physical attacks counter-measures). For details, see [54].

2.3.3 Application Functionalities

This application stores the personal information related to the cardholder of an MRTD or an IDL. It also allows governmental organizations to retrieve these pieces of data.
The applet supports the authentication mechanisms described in ICAO and EAC specifications and ISO/IEC 18013-3 ISO Compliant Driving License specification with a fully configurable access control management over the EFs (EFs).
The applet may be used on a contact mode (compliant to ISO/IEC 7816-3 specification) and/or contactless mode (compliant to ISO/IEC 14443 specification).
The compliancy of the applet to LDS, EAC, or IDL, is achieved provided a correct personalization is performed. The correct authentication mechanisms and access conditions over the EFs must be assigned.
In summary, the applet supports the following authentication mechanisms stated in the ICAO specifications (for MRTD) and the ISO Compliant Driving License standard (for IDL):

- Active Authentication (AA)
- Password Authenticated Connection Establishment (PACE)
- Chip Authentication (CA)
- Chip Authentication Mapping (CAM)

Each authentication mechanism is presented in the following chapters, all are part of the product but only some are part of the present evaluation.

2.3.3.1 Active Authentication (AA)

Active Authentication is an authentication mechanism ensuring the chip is genuine. It uses a challenge-response protocol between the IS and the chip.
Active Authentication is realized with the INTERNAL AUTHENTICATE command.
The key and algorithms supported are the following:

RSA ISO/IEC 9796-2 with a key length of 1024 bits, 1536 bits or 2048 bits and hashing algorithm of SHA1 or SHA2.
ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 and the key sizes 192 to 512.
AES-256 using ISO/IEC 9797-1 M2 padding method.
TDES with double and triple length keys using ISO/IEC 9797-1 M2 padding method.

2.3.3.2 Basic Access Control (BAC)

The protocol for Basic Access Control is specified by ICAO [47]. Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD. The protocol for Basic Access Control is based on ISO/IEC 11770-2 [41] key establishment mechanism 6. This protocol is also used to generate session keys that are used to protect the confidentiality (and integrity) of the transmitted data.
The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system Reads the printed data in the MRZ (for MRTD),
Authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.
The purpose of this mechanism is to ensure that the holder gives access to the IS to the logical MRTD (data stored in the chip); It is achieved by a mutual authentication.
Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.
This table lists the supported configurations for BAC protocol:

Configuration	Key Algo	Key Length	Hash Algo	MAC Algo
BAC	3DES 2Key	16-bytes	SHA-1	Retail MAC

Table 7: BAC Configuration

2.3.3.3 Terminal Authentication

The Terminal Authentication Protocol is a two move challenge-response protocol that provides explicit unilateral authentication of the terminal.
This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

2.3.3.4 Chip Authentication

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.
The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication is an alternative to the optional ICAO Active Authentication, i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:
Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
Besides authentication of the MRTD chip this protocol also provides strong session keys.
The protocol in version 1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.
The protocol in Version 2 provides explicit authentication of the MRTD chip by verifying the authentication token and implicit authentication of the stored data by performing Secure Messaging using the new session keys.

2.3.3.5 Password Authenticated Connection Establishment (PACE)

PACE is an access control mechanism that is supplemental to BAC. It is a cryptographically stronger access control mechanism than BAC since it uses asymmetric cryptography compared to BAC's symmetric cryptography.

PACE is realized through 5 commands:
1. MSE SET – AT command
2. GENERAL AUTHENTICATE command – Encrypted Nonce
3. GENERAL AUTHENTICATE command – Map Nonce
4. GENERAL AUTHENTICATE command – Perform Key Agreement
5. GENERAL AUTHENTICATE command – Mutual Authentication

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.
This table lists the supported configurations for PACE protocol:

Configuration	Mapping	Key Algo	Key Length (in bytes)	Secure Messaging	Auth. Token	Hash Algo
PACE–ECDH–GM–3DES	Generic	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE–ECDH–GM–AES–128	Generic	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–GM–AES–192	Generic	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–GM–AES–256	Generic	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–3DES	Integrated	3DES 2Key	16	CBC / Retail MAC	Retail MAC	SHA-1
PACE–ECDH–IM–AES–128	Integrated	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–IM–AES–192	Integrated	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–IM–AES–256	Integrated	AES	32	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–128	Chip Authentication	AES	16	CBC / CMAC	CMAC	SHA-1
PACE–ECDH–CAM–AES–192	Chip Authentication	AES	24	CBC / CMAC	CMAC	SHA-256
PACE–ECDH–CAM–AES–256	Chip Authentication	AES	32	CBC / CMAC	CMAC	SHA-256

Table 8: PACE Configuration

2.3.3.6 Extended Access Control (EAC)

EAC is an authentication protocol based on a PKI infrastructure. It further ensures that the IS is authorized to read and/or update data stored in the applet. This authentication mechanism generates a strong secure messaging session through the step of Chip Authentication.
This mechanism is realized by the following steps:
1. Chip Authentication (CA) Chip Authentication is achieved by using a MANAGE SECURITY ENVIRONMENT – SET – Key Agreement Template (MSE SET KAT) command or by using a MANAGE SECURITY ENVIRONMENT – SET – Authentication Template (MSE SET AT) command followed by GENERAL AUTHENTICATE command.

The Chip Authentication mechanism enables the authentication of the chip by using an authenticated DH scheme. It may be realized in two ways:

- Classical DH (DH El Gamal) with key length of 1024, 1536, or 2048 bits
- DH over Elliptic curves over prime fields (ECDH) with the key length supported by the underlying Java Card platform.

2. Certificate Chain Handling

The certificate chain is processed through a series of MANAGE SECURITY ENVIRONMENT – SET – Digital Signature Template (MSE SET DST) and PERFORM SECURITY OPERATION – Verify Certificate (PSO VERIFY) commands.
The chain is done to extract a key from the IS certificate, the key which will be used in the Terminal Authentication.
3. Terminal Authentication (TA)

Terminal Authentication is achieved by using an EXTERNAL AUTHENTICATE command.
The Terminal Authentication mechanism is an authentication of the IS based on a classical challenge/response scheme. The signature scheme may be:
ECDSA SHA-1, ECDSA SHA-224, ECDSA SHA-256, ECDSA SHA-384, or ECDSA SHA-512 on elliptic curves over prime field with key length supported by the underlying Java Card platform
RSA SHA-1, SHA-256, or SHA-512 (PKCS#1 v1.5 or PKCS#1 v2.1 - PSS) with a key length of 1024, 1536, and 2048 bits.

2.3.3.7 PACE-CAM

The Chip Authentication Mapping is a new mapping for PACE which extends the Generic Mapping that integrates Chip Authentication into the PACE protocol. This mapping combines PACE and Chip Authentication into one protocol PACE-CAM, which allows faster execution than the separate protocols (i.e. PACE + CA + TA).
PACE-CAM is realized the same way as § 2.3.3.6. The only difference is that the chip computes the Chip Authentication Data using the chip's static private key then sends this data to the terminal. The terminal verifies the authenticity of the chip using the recovered Chip Authentication Data.

2.3.3.8 Match On-Card (MOC) Verification

MOC verification may be used to grant some access rights to EFs.
This feature relies on the services provided by the CHV Server applet MOC verification is supported if the *CHV Configuration* is properly configured in the install parameter. Once the MOC verification is allowed the applet will permit the use of CHV-related commands that handles biometric and Global PIN credentials.

2.3.3.9 PIN

The product supports the management of card holder credentials such as Cardholder PIN and Global PIN which can be used to grant access rights to EFs or keys. The Cardholder PIN and Global PIN each have its PIN Unblocking Key (Cardholder PUK and Global PUK, respectively). These PINs and corresponding PUKs have to be initialized during personalization if they are used to protect access to EFs and keys.

2.3.3.10 BAC De-Activation

The TOE supports the automatic deactivation of BAC protocol at defined date.

2.3.3.11 Watermarking

The watermarking feature may be used to restrict the access to the plain image data of particular EF(s). Enabling the watermarking will cause the image data to be corrupted during the reading of the file contents.
The de-watermarking conditions should be configured accordingly and these conditions must be satisfied in order to grant access to the plain image data, details are in the dedicated security Target.

2.3.3.12 Secure Messaging

The TOE supports the ISO Secure Messaging. It provides a secure channel (i.e. encrypted and authenticated) between application and terminal. Secure Messaging can be set up by Chip Authentication, PACE, or Basic Access Control. The provided security level depends on the mechanism used to set up Secure Messaging.

A session is started when secure messaging is established. The session only ends with the release of secure messaging, e.g. by sending a command without secure messaging.

2.3.3.13 IDEMIA library

A dedicated cryptographic library has been developed and designed by IDEMIA.

This cryptographic library is embedded on the TOE to provide the highest security level and best tuned performances. It is implemented at the platform level and are already in the scope of the platform evaluation.

2.3.4 Mechanism included in the scope of the evaluation

All TOE functionalities are presented in the previous chapter.
The present evaluation includes the listed functionalities:

- PACE
- PACE-CAM
- AA
- CA

2.4 TOE Guidance

The TOE is identified as follows:

Application Guidance	
TOE name (commercial name)	LDS V10.1 on ID-One Cosmo v8.2 Platform
Guidance document for preparation	AGD_PRE [60]
Guidance document for operational use	AGD_OPE [61]
Platform Guidance	
Guidance document for Platform Pre-personalisation	COSMO V8.2 Pre-Perso Guide[57]
Developer of sensitive applications*	COSMO V8.2 Security Recommendations [56]
Guidance for application developer*	COSMO V8.2 Reference Guide [58]
Guidance to Issuer of the platform that aims to load applications*	COSMO V8.1-N Application Loading Protection Guidance [55]

Table 9: TOE Guidance

An ST Lite version of this Security Target will also serve as a guidance document.

3 TOE Life Cycle

3.1 TOE Life Cycle Overview

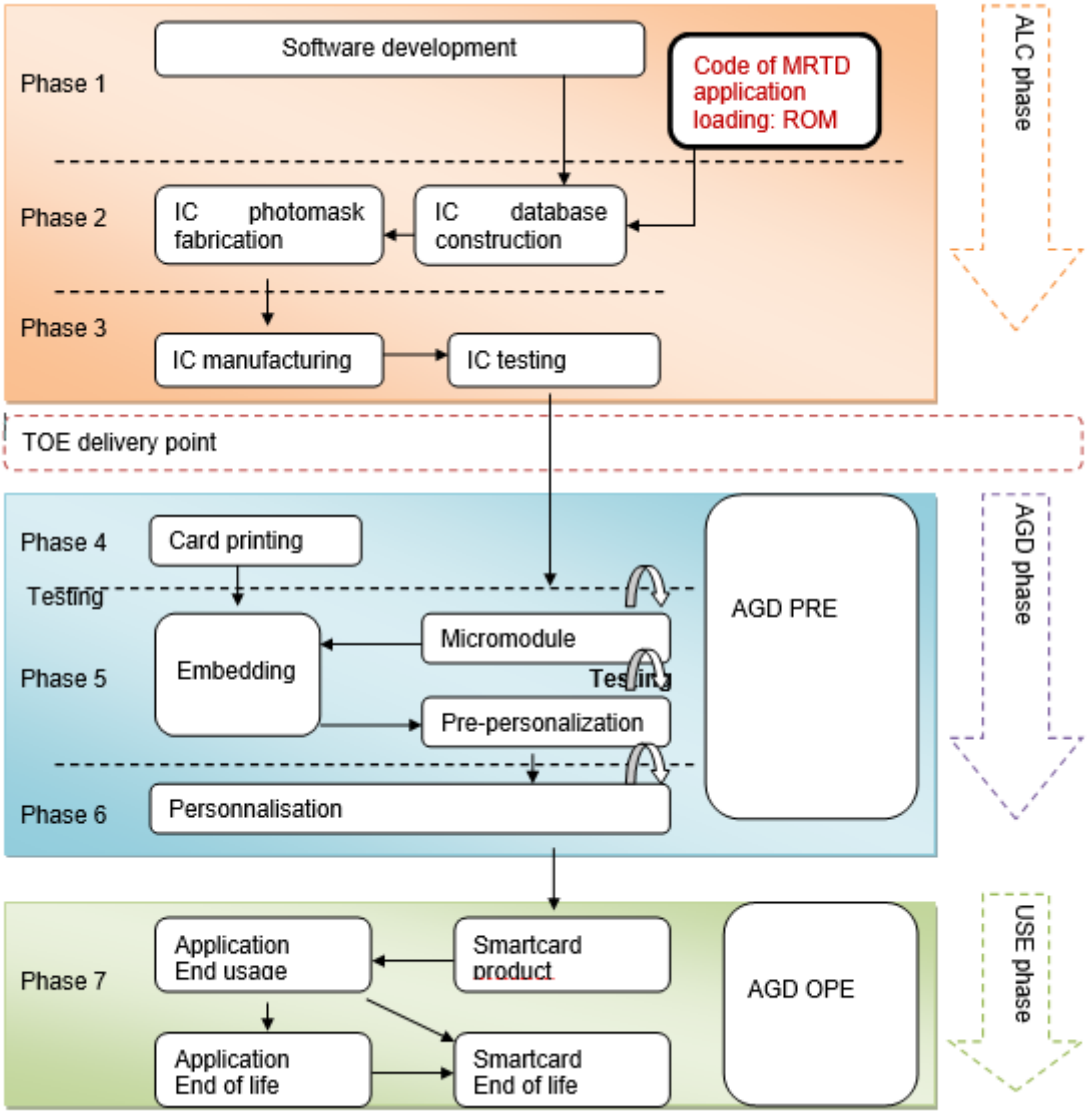

Figure 3: Smartcard product life-cycle for the TOE

The TOE life-cycle classically described in terms of four life-cycle phases is additionally subdivided into 7 steps.
The roles involved in the different steps are listed in the following table:

Roles	Subjects
IC manufacturer	NXP Semiconductors
TOE developer	IDEMIA
Manufacturer	NXP Semiconductors IDEMIA or another agent
Pre-personalizer	IDEMIA or another agent

Personalization Agent	IDEMIA or another agent

Table 10: Roles Identification on the life cycle.

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

Steps	Phase	Subject	Covered by
Step 1	Development	IDEMIA	ALC R&D sites
Step 2	Development	NXP Semiconductors	IC certification
Step 3	Manufacturing	NXP Semiconductors	IC certification
TOE delivery point			
Step 4	Manufacturing	MRTD Manufacturer (Pre-personalizer)	AGD_PRE
Step 5	Manufacturing	MRTD Manufacturer (Pre-personalizer)	AGD_PRE
Step 6	Personalization	Personalization Agent	AGD_PRE
Step 7	Operational Use	End user	AGD_OPE

Table 11: Subjects identification following life cycle steps

Details for each phase/step are presented in the following paragraphs.

3.2 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.

The TOE includes the LDS V10.1 application and the Platform.
The LDS and Platform are both developed at IDEMIA R&D sites.
The sites are audited following MSSR last requirements.

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

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

3.3 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 Manufacturer. The IC is securely delivered from the IC manufacture to the* Manufacturer. If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). The IC manufacturer adds initialization data in EEPROM and keys (MSK, LSK).

The end of step 3 is the TOE delivery.

(Step4) The 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 Manufacturer (i) adds the IC Embedded Software (ii) creates the eMRTD application, and (iii) equips travel document's chips with pre-personalization Data.

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

3.4 Phase 3 "Personalization of the travel document"

(Step6) The personalization of the travel document includes:
the survey of the travel document holder's biographical data,
(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
(iii) the personalization of the visual readable data onto the physical part of the travel document,
(iv) the writing of the TOE User Data and TSF Data into the logical travel document and
(v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of
(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2), and
(iii) the Document security object. The signing of the Document security object by the Document signer finalizes the personalization of the genuine travel document for the travel document holder.

The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

3.4.1 Loading of application

The platform can host 2 kinds of applications: Evaluated sensitive applications and validated basic applications. Once the application is evaluated or validated, it is securely delivered to manufacturing site. This delivery ensures the integrity and confidentiality of the application code and data. Then applications code and data are securely stored.

The delivery, storage and loading of any application are covered by audited Organisational measures (ALC).

Applications can be loaded at pre issuance at step 5 or at step 6 or in post issuance.

3.4.2 Applet pre-personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE. During this phase, the Java Card applet is prepared as required by P.TOE_Construction.
All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

3.4.3 TOE personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE, which is in charge of the Java Card applet personalisation.

All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Personalisation Agent is responsible for ensuring a sufficient level of security during this phase.

The Java Card applet is personalized according to guidance document [57].

At the end of phase 6, the TOE is constructed.

3.5 Phase 4 “Operational Use”

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

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

4 Conformance claims

4.1 Common Criteria conformance

This Security Target (ST) claims conformance to the Common Criteria version 3.1 revision 5 ([1][2][3]).
The conformance to the CC is claimed as follows:

CC	Conformance rationale
Part 1	Strict conformance
Part 2	Conformance to the extended[1] part: **1.** FAU_SAS.1 *"Audit Storage"* **2.** FCS_RND.1 *"Quality metric for random numbers"* **3.** FMT_LIM.1 *"Limited capabilities"* **4.** FMT_LIM.2 *"Limited availability"* **5.** FPT_EMS.1 *"TOE Emanation"* **6.** FIA_API.1 *"Authentication Proof of Identity"*
Part 3	Strict conformance to Part 3. The product claims conformance to EAL 5, augmented with: **1.** ALC_DVS.2 *"Sufficiency of security measures"* **2.** AVA_VAN.5 "Advanced methodical vulnerability analysis"

Table 12: Conformance Rationale

4.2 Protection Profile conformance

The Security Target claims strict conformance to the following PP written in CC3.1 revision 3:
BSI-CC-PP-0068-V2-2011:"Machine Readable Travel Document using Standard Inspection Procedure with PACE" [50].

4.3 Protection Profile additions

The rationale between the SPD, taking into account the additional elements of the SPD, and the Objectives and Objectives on the operational environment are given in the paragraph Rationales.

4.3.1 SFR dispatch versus PP

The following table present a rationale between the SFR driven from the protection profile versus the SFR from this security target:

SFR from the PP	Dispatch in the ST
FCS_CKM.1/DH_PACE	FCS_CKM.1/ECDH_PACE_AES FCS_CKM.1/ECDH_PACE_3DES
FCS_CKM.4	FCS_CKM.4/Global
FCS_COP.1/PACE_ENC	FCS_COP.1/PACE_ENC_3DES FCS_COP.1/PACE_ENC_AES
FCS_COP.1/PACE_MAC	FCS_COP.1/PACE_MAC_AES FCS_COP.1/PACE_MAC_3DES
FCS_RND.1	FCS_RND.1/Global
FIA_AFL.1/PACE	FIA_AFL.1/PACE
FIA_UID.1/PACE	FIA_UID.1/PACE
FIA_UAU.1/PACE	FIA_UAU.1/PACE
FIA_UAU.4/PACE	FIA_UAU.4/PACE
FIA_UAU.5/PACE	FIA_UAU.5/PACE
FIA_UAU.6/PACE	FIA_UAU.6/PACE
FDP_ACC.1/TRM	FDP_ACC.1/TRM

1 The rationale for SFR addition is described in the relative PP

SFR from the PP	Dispatch in the ST
FDP_ACF.1/TRM	FDP_ACF.1/TRM
FDP_RIP.1	FDP_RIP.1
FDP_UCT.1/TRM	FDP_UCT.1/TRM
FDP_UIT.1/TRM	FDP_UIT.1/TRM
FTP_ITC.1/PACE	FTP_ITC.1/PACE
FAU_SAS.1	FAU_SAS.1
FMT_SMF.1	FMT_SMF.1
FMT_SMR.1/PACE	FMT_SMR.1/PACE
FMT_LIM.1	FMT_LIM.1/Global
FMT_LIM.2	FMT_LIM.2/Global
FMT_MTD.1/INI_ENA	FMT_MTD.1/INI_ENA
FMT_MTD.1/INI_DIS	FMT_MTD.1/INI_DIS
FMT_MTD.1/KEY_READ	FMT_MTD.1/PACE_KEY_READ
FMT_MTD.1/PA	FMT_MTD.1/PA
FPT_EMS.1	FPT_EMS.1/Global FPT_EMS.1/PACE
FPT_FLS.1	FPT_FLS.1/Global
FPT_TST.1	FPT_TST.1/Global FPT_TST.1/PACE FPT_TST.1/CA
FPT_PHP.3	FPT_PHP.3.1/Global

Table 13: PP SFR

4.3.2 Overview of the SFR defined in this ST

SFR are presented in **§ 8.1 Security Functional Requirements**:

1. SFR (**/Global**) that are global to the product (shared between the various TOE)
2. SFR (**/AA**) that are dedicated for Active Authentication
3. SFR (**/PACE**) that are dedicated for PACE protocol
4. SFR (**/PACE_CAM**) that are dedicated for Password Authenticated Connection Establishment with Chip Authentication Mapping

4.3.2.1 Complete overview of the SFR

The following table presents all the SFR defined in the ST with the generic notation.

SFR from the PP
FCS_CKM.1/DH_PACE ; FCS_CKM.4; FCS_COP.1/PACE_ENC ; FCS_COP.1/PACE_MAC; FCS_RND.1; FIA_AFL.1/PACE; FIA_UID.1/PACE ; FIA_UAU.1/PACE ; FIA_UAU.4/PACE ; FIA_UAU.5/PACE ; FIA_UAU.6/PACE ; FDP_ACC.1/TRM ; FDP_ACF.1/TRM ; FDP_RIP.1 ; FDP_UCT.1/TRM; FDP_UIT.1/TRM ; FAU_SAS.1 ; FMT_SMF.1 ; FMT_SMR.1/PACE ; FMT_LIM.1 ; FMT_LIM.2 ; FMT_MTD.1/INI_ENA ; FMT_MTD.1/INI_DIS ; FMT_MTD.1/KEY_READ ; FMT_MTD.1/PA ; FPT_EMS.1 ; FPT_FLS.1 ; FPT_TST.1 ; FPT_PHP.3

Table 14: SFR from the PP

Section	Additional SFR
Active Authentication	FCS_COP.1/AA ; FDP_DAU.1/AA ; FDP_ITC.1/AA ; FMT_MTD.1/AA_KEY_READ ; FMT_MOF.1/AA ; FMT_MTD.1/AA_KEY_WRITE
Chip Authentication	FIA_API.1/CA ; FSC_CKM.1/CA ; FCS_COP.1/CA ; FIA_UAU.1/CA ; FIA_UAU.5/CA ; FIA_UAU.6/CA ; FIA_UID.1/CA ; FPT_TST.1/CA ; FMT_MTD.1/CA_KEY_WRITE ; FMT_MTD.1/CA_KEY_READ ; FDP_UCT.1/CA ; FDP_UIT.1/CA
PACE_CAM	FIA_UAU.1/PACE_CAM; FIA_UAU.4/PACE_CAM; FIA_UAU.5/PACE_CAM; FIA_UAU.6/PACE_CAM; FIA_UID.1/PACE_CAM; FMT_MTD.1/CA_KEY_WRITE

Table 15: Additional SFR

4.3.2.2 Global SFR overview

Global SFR	Additional?	ST generic notation
FCS_CKM.4/Global	No	FCS_CKM.4
FCS_RND.1/Global	No	FCS_RND.1
FMT_LIM.1/Global	No	FMT_LIM.1
FMT_LIM.2/Global	No	FMT_LIM.2
FPT_EMS.1/Global	No	FPT_EMS.1
FPT_FLS.1/Global	No	FPT_FLS.1
FPT_TST.1/Global	No	FPT_TST.1
FPT_PHP.3/Global	No	FPT_PHP.3

Table 16: Global SFR overview

4.3.2.3 Active Authentication SFR overview

Active Auth. SFR	Additional?	ST generic notation
FCS_COP.1/AA_DSA FCS_COP.1/AA_ECDSA	Yes	FCS_COP.1/AA
FDP_DAU.1/AA	Yes	FDP_DAU.1/AA
FDP_ITC.1/AA	Yes	FDP_ITC.1/AA
FMT_MTD.1/AA_KEY_READ	Yes	FMT_MTD.1/AA_KEY_READ
FPT_EMS.1/AA	No	FPT_EMS.1
FMT_MOF.1/AA	Yes	FMT_MOF.1/AA
FMT_MTD.1/AA_KEY_WRITE	Yes	FMT_MTD.1/AA_KEY_WRITE

Table 17: Additional SFR for the Active Authentication

4.3.2.4 PACE SFR overview

PACE SFR	Additional?	ST generic notation
FCS_CKM.1/ECDH_PACE_AES FCS_CKM.1/ECDH_PACE_3DES	No	FCS_CKM.1/DH_PACE
FCS_COP.1/PACE_ENC_AES FCS_COP.1/PACE_ENC_3DES	No	FCS_COP.1/PACE_ENC
FCS_COP.1/PACE_MAC_AES FCS_COP.1/PACE_MAC_3DES	No	FCS_COP.1/PACE_MAC
FDP_ACC.1/TRM	No	FDP_ACC.1/TRM
FDP_ACF.1/TRM	No	FDP_ACF.1/TRM
FDP_RIP.1	No	FDP_RIP.1
FDP_UCT.1/TRM	No	FDP_UCT.1/TRM
FDP_UIT.1/TRM	No	FDP_UIT.1/TRM
FIA_AFL.1/PACE	No	FIA_AFL.1/PACE
FIA_UAU.1/PACE	No	FIA_UAU.1/PACE
FIA_UAU.4/PACE	No	FIA_UAU.4/PACE
FIA_UAU.5/PACE	No	FIA_UAU.5/PACE
FIA_UAU.6/PACE	No	FIA_UAU.6/PACE
FIA_UID.1/PACE	No	FIA_UID.1/PACE
FMT_MTD.1/PACE_KEY_READ	No	FMT_MTD.1/PACE_KEY_READ
FMT_SMR.1/PACE	No	FMT_SMR.1/PACE
FPT_EMS.1/PACE	No	FPT_EMS.1
FTP_ITC.1/PACE	No	FTP_ITC.1/PACE
FPT_TST.1/PACE	No	FPT_TST.1/PACE
FMT_MTD.1/PA	No	FMT_MTD.1/PA

Table 18: PACE SFR overview

4.3.2.5 CA SFR overview

CA SFR	Additional?	ST generic notation
FIA_API.1/CA	Yes	FIA_API.1/CA

FCS_CKM.1/CA_DH_SM_3DES FCS_CKM.1/CA_ECDH_SM_3DES FCS_CKM.1/CA_DH_SM_AES FCS_CKM.1/CA_ECDH_SM_AES	Yes	FCS_CKM.1/CA
FCS_COP.1/CA_SHA_SM_3DES FCS_COP.1/CA_SYM_SM_3DES FCS_COP.1/CA_MAC_SM_3DES FCS_COP.1/CA_SHA_SM_AES FCS_COP.1/CA_SYM_SM_AES FCS_COP.1/CA_MAC_SM_AES	Yes	FCS_COP.1/CA
FDP_ITC.1/CA	Yes	FDP_ITC.1/CA
FIA_UAU.1/CA	Yes	FIA_UAU.1/CA
FIA_UAU.5/CA_3DES FIA_UAU.5/CA_AES	Yes	FIA_UAU.5/CA
FIA_UAU.6/CA	Yes	FIA_UAU.6/CA
FIA_UID.1/CA	Yes	FIA_UID.1/CA
FPT_EMS.1/CA	No	FPT_EMS.1
FPT_TST.1/CA	Yes	FPT_TST.1/CA
FMT_MTD.1/CA_KEY_WRITE	Yes	FMT_MTD.1/CA_KEY_WRITE
FMT_MTD.1/CA_KEY_READ	Yes	FMT_MTD.1/CA_KEY_READ
FDP_UCT.1/CA	Yes	FDP_UCT.1/CA
FDP_UIT.1/CA	Yes	FDP_UIT.1/CA

Table 19: CA SFR overview

4.3.3 Overview of the additional protocols

4.3.3.1 Chip Authentication

The Chip Authentication has been added to this Security Target in order to reinforce the BAC authentication mechanism by ensuring the verification of the Card by the Terminal. For this addition, the TOE SPD has been refined and contains the following additions:

1. Additional Threats: **§ 6.3.2**
2. Additional Objective: **§ 7.1.2**
3. Additional OSP: **§ 6.4.2**
4. Additional Assumptions: **§ 6.5.3**

4.3.3.2 Active Authentication

The additional functionality of Active Authentication (AA) is based on the ICAO PKI V1.1 and the related on-card generation of RSA and ECC keys.
It implies the following addition to the standard PP:

1. Additional Threats: **§ 6.3.3**
2. Additional Objective: **§ 7.1.3**
3. Additional OSP: **§ 6.4.3**
4. Additional Assumptions: **§ 6.5.2**

4.3.3.3 Prepersonalization phase

The prepersonalization phase has been reinforced in this Security Target, with the following elements.
This functionality is usable in phase 5 and phase 6. Once the product is locked, stated as personalized, it is no more possible to perform this operation.
Rationale for the additions
In order to be compliant with the CEM, a rationale is given for the additional Objectives on the Environment, such as to demonstrate that they neither mitigates a threat nor fulfil an OSP.

4.3.4 OE for CA rationale

OE.Exam_MRTD_CA, OE.Prot_Logical_MRTD_CA and **OE.Auth_Key_MRTD** define additional requirements on the operational environment for the Chip Authentication Protocol which is not in the original scope of the PP BAC. This OE is only linked to threat and OSP for the Chip Authentication and has no links with those of the PP.

4.3.5 OE for AA rationale

The objectives **OE.Exam_MRTD_AA, OE.Prot_Logical_MRTD_AA, OE.Activ_Auth_Verif** and **OE.Activ_Auth_Sign** define additional requirements on the operational environment for the Active Authentication Protocol which is not in the original scope of the PP BAC. This OE is only linked to threat and OSP for the Active Authentication and has no links with those of the PP.

4.3.6 Assumption for AA rationale

The A.Insp_Sys_AA **is added,** this assumption is only linked to Active Authentication mechanism as the Inspection System has to implement the mechanism and shall verifiy the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

4.3.7 Assumption for CA rationale

The A.Insp_Sys_CA,

The assumption **A.Insp_Sys_CA** serves only the Chip authentication mechanism added in the scope of the evaluation. The inspection system shall implement the CA mechanism. The IS has to verify the authenticity of the MRTD during the inspection by establishing a secure messaging.

A.Signature_PKI

This assumption is only linked to the Chip authentication as the issuing and receiving States or Organizations shall establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD.

5 Security problem definition

5.1 Subjects

SFR	Before phase 5	Phase 5	Phase 6	Phase 7
PP PACE subjects				
Travel Document Holder				x
Travel Document Presenter				x
Terminal		x	x	x
Basic Inspection System with PACE				x
Document Signer			x	x
Country Signing Certification Authority			x	x
Personalization Agent			x	
Manufacturer	x	x		
Attacker	x	x	x	x

Table 20: Subjects and phases

5.1.1 PP PACE subjects

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 phase25. 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 [47].

Personalization Agent

An organization acting on behalf of the travel document Issuer to personalize 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 personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [43],

(iv) writing the document details data,

(v) writing the initial TSF data,

(vi) signing the Document Security Object defined in [43] (in the role of DS).

Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.

This entity is commensurate with ‘Personalization agent’ in [47].

Application Note:
Personalization Agent is referred as the Personalizer in the Security Target

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 [47].

Basic Inspection System with PACE (BIS-PACE)

A technical system being used by an inspecting authority and verifying the travel document presenter as the travel document holder (for *ePassport*: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).
BIS-PACE implements the terminal’s part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.

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 authorized by the national CSCA issuing the Document Signer Certificate see [43].This role is usually delegated to a Personalization Agent.

Country Signing Certification Authority (CSCA)

An organization 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 having to be distributed by strictly secure diplomatic means, see [43].

Travel document holder (MRTD holder)
A person for whom the travel document Issuer has personalized the travel document. This entity is commensurate with ‘MRTD Holder’ in [47]. Please note that a travel document holder can also be an attacker.

Travel document presenter (Traveler)
A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with ‘Traveler’ in [47]. Please note that a travel document presenter can also be an attacker.

Attacker
A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, 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 recognized by the TOE.
This external entity is commensurate with ‘Attacker’ in [47].

5.2 Assets

5.2.1 Primary assets

All these primary assets represent User Data in the sense of the Common Criteria. Please note that user data being referred in this chapter include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy

defined by the current ST also secures these specific travel document holder's data as stated in this chapter.

User data stored on the TOE
Protection: Confidentiality, Integrity, Authenticity
All data (being not authentication data) stored in the context of the eMRTD application of the travel document as defined in [53] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [53])
This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [47].

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

Table 21: User data stored on the TOE

User data transferred between the TOE and the terminal connected
Protection: Confidentiality, Integrity, Authenticity
All data (being not authentication data) being transferred in the context of the eMRTD application of the travel document between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [53]).
User data can be received and sent (exchange <--> [receive, send]).

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

5.2.2 Secondary assets

Accessibility to the TOE functions and data only for authorized subjects
Protection: Availability
Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.

Genuineness of the TOE
Protection: Availability
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 chip'' in [47].

TOE internal secret cryptographic keys
Protection: Confidentiality, Integrity
Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

TSF data	Description
Personalisation Agent reference authentication Data	Private key enabling to authenticate the Personalisation agent
Password Authenticated Connection Establishment (PACE) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document

TSF data	Description
Chip Authentication private Key	Private key the chip uses to perform a chip authentication
Active Authentication private key	Private key the chip uses to perform an active authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity

Table 22: TOE internal secret cryptographic keys

TOE internal non-secret cryptographic material

Protection: Authenticity, Integrity

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.

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

Table 23: TOE internal non-secret cryptographic material

Travel Document communication establishment authorization data

Protection: Confidentiality, Integrity

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

TSF data	Description
PACE password (MRZ or CAN)	Reference information being persistently stored in the TOE and allowing PACE authentication

Table 24: Travel Document communication establishment authorization data

5.3 Threats

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

5.3.1 Threats from the PP PACE

T.Skimming

Adverse action

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

Threat agent

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

Asset

Confidentiality of logical travel document data

T.Eavesdropping

Adverse action

An attacker is listening to the communication between the travel document and the 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

T.Tracing

Adverse action

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

Threat agent

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

Asset

Privacy of the travel document holder

T.Forgery

Adverse action

An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the 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.

T.Abuse-Func

Adverse action

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

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

This threat addresses the misuse of the functions for the initialization and the personalization in the operational phase after delivery to MRTD holder.

Threat agent

Having high attack potential, being in possession of one or more legitimate MRTD.

Asset

Integrity and authenticity of logical MRTD, availability of the functionality of the MRTD.

T.Information_Leakage

Adverse action

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

Threat agent

Having high attack potential

Asset

Confidentiality of User Data and TSF data of the travel document

T.Phys-Tamper

Adverse action

An attacker may perform physical probing of the MRTD's chip in order to

(i) Disclose TSF Data or
(ii) Disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip 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 MRTD

Threat agent
Having high attack potential, being in possession of a legitimate MRTD.
Asset
Integrity and authenticity of logical MRTD, availability of the functionality of the MRTD, confidentiality of User Data and TSF-data of the MRTD

T.Malfunction
Adverse action
An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to
(i) Deactivate or modify security features or functions of the TOE
(ii) Circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.
This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. 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 MRTD, 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

5.3.2 Threats for CA and AA

T.Counterfeit
Adverse action
An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveller by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.
Threat agent
having high attack potential, being in possession of one or more legitimate MRTDs
Asset
authenticity of logical MRTD data

5.4 Organisational Security Policies

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

5.4.1 OSP from PP PACE

P.Manufact
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

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

P.Card_PKI

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

2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [43]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer.

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
   (iv) Securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworthy_PKI

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

P.Terminal

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

1) The related terminals shall be used by terminal operators and by travel document holders
2) They shall implement the terminal parts of the PACE protocol [43], of the Passive Authentication [53] and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann)
3) The related terminals need not to use any own credentials
4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [53])
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

5.4.2 OSP for CA

P.Chip_Auth

The terminal implements the Chip Authentication protocol as described in [48].

5.4.3 OSP for AA

P.Activ_Auth
The terminal implements the Active Authentication protocol as described in [48].

5.5 Assumptions

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

5.5.1 Assumptions from PP PACE

A.Passive_Auth
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
(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 [43].

5.5.2 Assumptions for Active Authentication

A.Insp_Sys_AA
The Inspection System implements the Active Authentication Mechanism. The Inspection System verifies the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

5.5.3 Assumptions for Chip Authentication

A.Insp_Sys_CA
The Inspection System implements the Chip Authentication Mechanism. The Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism.

A.Signature_PKI
The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer

(i) generates the Document Signer Key Pair,
(ii) hands over the Document Signer Public Key to the CA for certification,
(iii) keeps the Document Signer Private Key secret and
(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs.

The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

6 Security Objectives

6.1 Security Objectives for the TOE

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

6.1.1 SO from PP PACE

OT.Data_Int
The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized 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_Auth
The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side.
The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Conf
The TOE must ensure confidentiality of the User Data and the TSF-data 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
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.CA_Proof (proof of travel document authenticity) cannot be achieved by the current TOE.

OT.Prot_Abuse-Func
The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order:

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

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

1. 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
2. Forcing a malfunction of the TOE and/or
3. 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
The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software by means of:

1. Measuring through galvanic contacts representing a direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
2. 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)
3. Manipulation of the hardware and its security features, as well as
4. Controlled manipulation of memory contents (User Data, TSF Data)

With a prior

5. Reverse-engineering to understand the design and its properties and functions.

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

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

OT.AC_Pers
The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [43] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization.

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

6.1.2 SO for CA

OT.CA_Proof
The TOE must support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [43]. The authenticity proof provided by the MRTD's chip shall be protected against attacks with high attack potential.

Application note: The objective implies the MRTD's to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [43] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.Data_Int_CA

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

6.1.3 SO for AA

OT.AA_Proof
The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD’s chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [43]. The authenticity proof through AA provided by MRTD’s chip shall be protected against attacks with high attack potential.

OT.Data_Int_AA
The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Active Authentication.

6.2 Security objectives for the Operational Environment

6.2.1 OE from PP PACE

6.2.1.1 Travel document Issuer as the general responsible

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

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

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

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

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

A Document Signer acting in accordance with the CSCA policy must:

(i) generate a cryptographically secure Document Signing Key Pair
(ii) ensure the secrecy of the Document Signer Private Key
(iii) hand over the Document Signer Public Key to the CSCA for certification
(iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [43].

The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [43]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalization
The travel document Issuer must ensure that the Personalization Agents acting on his behalf:

(i) Establish the correct identity of the travel document holder and create the biographical data for the travel document
(ii) Enroll the biometric reference data of the travel document holder
(iii) write a subset of these data on the physical Passport (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [43]
(iv) write the document details data
(v) write the initial TSF data
(vi) sign the Document Security Object defined in [43] (in the role of a DS).

OE.Terminal
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 [43]

2.) The related terminals implement the terminal parts of the PACE protocol of the Passive Authentication (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonce, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann)
3.) The related terminals need not to use any own credentials
4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [43])
5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

OE.Travel_Document_Holder
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.

6.2.2 OE for CA

OE.Auth_Key_MRTD
The issuing State or Organization has to establish the necessary public key infrastructure in order to:

1. Generate the MRTD's Chip Authentication Key Pair
2. Sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14
3. 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 Chip Authentication Public Key by means of the Document Security Object.

OE.Exam_MRTD_CA
Aditionally to the OE.Exam_MRTD, the inspection systems perform the Chip Authentication protocol to verify the Authenticity of the presented MRTD’s chip.

OE.Prot_Logical_MRTD_CA
Aditionally to the OE.Prot_Logical_MRTD, the inspection system prevents eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

6.2.3 OE for AA

OE.Exam_MRTD_AA
Aditionally to the OE.Exam_MRTD, the inspection systems perform the Active Authentication protocol to verify the Authenticity of the presented MRTD’s chip.

OE.Prot_Logical_MRTD_AA
Aditionally to the OE.Prot_Logical_MRTD, the inspection system prevents eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Active Authentication Protocol.

OE.Activ_Auth_Verif
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.

OE.Activ_Auth_Sign
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.

7 Extended requirements

7.1 Extended family FAU_SAS - Audit data storage

7.1.1 Extended components FAU_SAS.1

Description: see [50].
FAU_SAS.1 Audit storage
FAU_SAS.1.1 The TSF shall provide [assignment: authorized users] with the capability to store [assignment: list of audit information] in the audit records.

Dependencies: No dependencies.

Rationale: see [50]

7.2 Extended family FCS_RND - Generation of random numbers

7.2.1 Extended component FCS_RND.1

Description: see [50]
FCS_RND.1 Quality metric for random numbers
FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

Rationale: See [50]

7.3 Extended family FIA_API – Authentication proof of identity

7.3.1 Extended component FIA_API.1

Description: see [50]
FIA_API.1 Quality metric for random numbers
FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

Dependencies: No dependencies.

Rationale: See [50]

7.4 Extended family FMT_LIM - Limited capabilities and availability

7.4.1 Extended component FMT_LIM.1

Description: see [50]
FMT_LIM.1 Limited capabilities
FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.2)

Rationale: See [50]

7.4.2 Extended component FMT_LIM.2

Description: See [50]
FMT_LIM.2 Limited availability
FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: (FMT_LIM.1)

Rationale: See [50]

7.5 Extended family FPT_EMS - TOE Emanation

7.5.1 Extended component FPT_EMS.1

Description: see [50]
FPT_EMS.1 TOE Emanation
FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

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

Dependencies: No dependencies.

Rationale: See [50]

8 Security Requirements

8.1 Security Functional Requirements

This chapter presents the Security Functional Requirements to take into account within the TOE configuration presented in this security target. It is composed of the following elements:

1. **Global SFR** that are applicable to all the passports configuration
2. **Active Authentication SFR** that cover the Active Authentication Protocol
3. **CA SFR** that cover the Chip Authentication Protocol
4. **PACE SFR** that cover the Password Authenticated Connection Establishment protocol
5. **PACE CAM** that cover the Password Authenticated Connection Establishment with Chip Authentication Mapping protocol

8.1.1 Global SFR

This chapter covers the common SFR that are shared between the different applications that are embedded on the product.

FCS_CKM.4/Global Cryptographic key destruction

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

FCS_RND.1/Global Quality metric for random numbers

FCS_RND.1.1/Global The TSF shall provide a mechanism to generate random numbers that meet

1. Deterministic Hybrid random number as defined in [54]
2. The requirement of FIPS SP800-90 [18] for random number generation.

FMT_LIM.1/Global Limited capabilities

FMT_LIM.1.1/Global The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow

1. **User Data to be manipulated**
2. **TSF data to be disclosed or manipulated**
3. **Software to be reconstructed**
4. **Substantial information about construction of TSF to be gathered which may enable other attacks**

FMT_LIM.2/Global Limited availability

FMT_LIM.2.1/Global The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced**:**
Deploying Test Features after TOE Delivery does not allow

1. **User Data to be manipulated**
2. **TSF data to be disclosed or manipulated**
3. **Software to be reconstructed**
4. **Substantial information about construction of TSF to be gathered which may enable other attacks**

FPT_EMS.1/Global TOE Emanation

FPT_EMS.1.1/Global The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

1. **EF.COM, EF.SOD and EF.DG1 to EF.DG16**

FPT_EMS.1.2/Global The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to

1. **EF.COM, EF.SOD and EF.DG1 to EF.DG16**

FPT_FLS.1/Global Failure with preservation of secure state

FPT_FLS.1.1/Global The TSF shall preserve a secure state when the following types of failures occur:

1. **Exposure to out-of-range operating conditions where therefore a malfunction could occur**
2. **Failure detected by TSF according to FPT_TST.1.**

FPT_TST.1/Global TSF testing

FPT_TST.1.1/Global The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**

1. **At reset**

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

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

FPT_PHP.3/Global Resistance to physical attack

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

8.1.2 Active Authentication SFR

FCS_COP.1/AA_DSA Cryptographic operation

FCS_COP.1.1/AA_DSA The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following **[standard]**:

Operation	Algorithm	Key length (bits)	Standard
Digital Signature Creation	**RSA signature (CRT or SFM) with SHA1, 224, 256, 384, 512**	**1024 to 2048 with a step of 256 bits**	**[24]**

FCS_COP.1/AA_ECDSA Cryptographic operation

FCS_COP.1.1/AA_ECDSA The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following **[standard]**:

Operation	Algo	Key length (bits)	Standard
Digital Signature Creation	**ECDSA with SHA1, 224, 256, 384, 512**	**192 to 521 over prime field curves**	**[24][28][29][30]**

FDP_DAU.1/AA Basic Data Authentication

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

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

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

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

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

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

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

FMT_MTD.1/AA_KEY_READ Management of TSF data

FMT_MTD.1.1/AA_KEY_READ The TSF shall restrict the ability to **read** the **AAK** to **none**.

FPT_EMS.1/AA TOE Emanation

FPT_EMS.1.1/AA The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

1. **Active Authentication: Private Key (AAK)**

FPT_EMS.1.2/AA The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to

1. **Active Authentication: Private Key (AAK)**

FMT_MOF.1/AA Management of security functions behaviour

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

FMT_MTD.1/AA_KEY_WRITE Management of TSF data

FMT_MTD.1.1/AA_KEY_WRITE The TSF shall restrict the ability to **write** the **AAK** to **Personalization Agent**.

8.1.3 Chip Authentication SFR

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication protocol according to** [45] to prove the identity of the **TOE**.

FCS_CKM.1/CA_DH_SM_3DES Cryptographic key generation

FCS_CKM.1.1/CA_DH_SM_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	**112**	**[43]**

FCS_CKM.1/CA_DH_SM_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	**128, 192, 256**	**[43]**

FCS_CKM.1/CA_ECDH_SM_3DES Cryptographic key generation

FCS_CKM.1.1/CA_ECDH_SM_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	**112**	**[43]**

FCS_CKM.1/CA_ECDH_SM_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	**128, 192, 256**	**[43]**

FCS_COP.1/CA_SHA_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_SHA_SM_3DES The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
SHA1	**None**	**[29]**

FCS_COP.1/CA_SHA_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_SHA_SM_AES The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length	Standards

	(bits)	
SHA1 and SHA256	None	[29]

FCS_COP.1/CA_SYM_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_SYM_SM_3DES The TSF shall perform **SM encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
3DES CBC mode	112	[29]

FCS_COP.1/CA_SYM_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_SYM_SM_AES The TSF shall perform **SM encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
AES	128, 192 and 256	[29]

FCS_COP.1/CA_MAC_SM_3DES Cryptographic key generation

FCS_COP.1.1/CA_MAC_SM_3DES The TSF shall perform **SM message authentication code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
3DES Retail MAC	112	[29]

FCS_COP.1/CA_MAC_SM_AES Cryptographic key generation

FCS_COP.1.1/CA_MAC_SM_AES The TSF shall perform **SM message authentication code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
AES CMAC	128, 192 and 256	[29]

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

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

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

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

FIA_UAU.1/CA Timing of authentication

FIA_UAU.1.1/CA The TSF shall allow:

1. **To establish the communication channel**
2. **To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS**
3. **To identify themselves by selection of the authentication key**
4. **To carry out the Chip Authentication Protocol**

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

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

FIA_UAU.5/CA_3DES Multiple authentication mechanisms

FIA_UAU.5.1/CA_3DES The TSF shall provide

1. **Secure Messaging in MAC-ENC mode**
2. **Symmetric Authentication Mechanism based on 3DES**

to support user authentication.

FIA_UAU.5.2/CA_3DES The TSF shall authenticate any user's claimed identity according to the

1. **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism**

FIA_UAU.5/CA_AES Multiple authentication mechanisms

FIA_UAU.5.1/CA_AES The TSF shall provide

1. **Secure Messaging in MAC-ENC mode**
2. **Symmetric Authentication Mechanism based on AES**

to support user authentication.

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

1. **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism**

FIA_UAU.6/CA Re-authenticating

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

FIA_UID.1/CA Timing of identification

FIA_UID.1.1/CA The TSF shall allow

1. **To establish the communication channel**
2. **To read the Initialization Data if it is not disbled by TSF according to FMT_MTD.1/INI_DIS**
3. **To carry out th Chip Authentication Protocol**

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

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

FPT_EMS.1/CA TOE Emanation

FPT_EMS.1.1/CA The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

1. **Chip Authentication: Session Keys, Private Key (CAK)**

FPT_EMS.1.2/CA The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to

1. **Active Authentication: Session Keys, Private Key (CAK)**

FPT_TST.1/CA TSF testing

FPT_TST.1.1/CA The TSF shall run a suite of self tests to demonstrate the correct operation of **the TSF, at the conditions:**

1. **At Reset**

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

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

FMT_MTD.1/CA_KEY_WRITE Management of TSF data

FMT_MTD.1.1/CA_KEY_WRITE The TSF shall restrict the ability to **write** the **CAK** to **Personalization Agent**.

FMT_MTD.1/CA_KEY_READ Management of TSF data

FMT_MTD.1.1/CA_KEY_READ The TSF shall restrict the ability to **read** the **CAK** to **none**.

FDP_UCT.1/CA Basic data exchange confidentiality

FDP_UCT.1.1/CA [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorized disclosure **after Chip Authentication protocol**.

FDP_UIT.1/CA Data exchange integrity

FDP_UIT.1.1/CA [Editorially Refined] The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors **after Chip Authentication protocol**

FDP_UIT.1.2/CA [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred **after Chip Authentication protocol**

8.1.4 PACE SFR

FCS_CKM.1/ECDH_PACE_3DES Cryptographic key generation

FCS_CKM.1.1/ECDH_PACE_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards

DH key derivation protocol compliant to PKCS#3	**3DES 2 keys**	**[43]**

FCS_CKM.1/ECDH_PACE_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
DH key derivation protocol compliant to ISO 15946	**128, 192 & 256**	**[43]**

FCS_COP.1/PACE_ENC_AES Cryptographic key generation

FCS_COP.1.1/PACE_ENC_AES The TSF shall perform **Secure Messaging - encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
AES in CBC mode	**128, 192 and 256**	**[17]**

FCS_COP.1/PACE_ENC_3DES Cryptographic key generation

FCS_COP.1.1/PACE_ENC_3DES The TSF shall perform **Secure Messaging - encryption and decryption** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
3DES in CBC mode	**112**	**[12]**

FCS_COP.1/PACE_MAC_AES Cryptographic key generation

FCS_COP.1.1/PACE_MAC_AES The TSF shall perform **Secure Messaging - Message Authentication Code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
CMAC AES	**128, 192 and 256**	**[17]**

FCS_COP.1/PACE_MAC_3DES Cryptographic key generation

FCS_COP.1.1/PACE_MAC_3DES The TSF shall perform **Secure Messaging - Message Authentication Code** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic algorithm	Key length (bits)	Standards
Retail MAC with 3DES	**112**	**[12]**

FDP_ACC.1/TRM Complete access control

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

FDP_ACF.1/TRM Security attribute based access control

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

1. **Subjects:**
   a. **Terminal**
   b. **BIS-PACE**
2. **Objects:**
   a. **Data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 EF.SOD and EF.COM of the logical MRTD**
   b. **Data in EF.DG3 of the logical MRTD**
   c. **Data in EF.DG4 of the logical MRTD**
   d. **All TOE intrinsic secret cryptographic keys stored in the 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.1.1/TRM according to [53] after a successful PACE authentication a required by FIA_UAU.1/PACE**

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

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the 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.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to and de-allocation of the resource from** the following objects:

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

FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD

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

FDP_UIT.1/TRM Data exchange integrity

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

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **10** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password**

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

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

1. **To establish the communication channel**
2. **Carrying out the PACE Protocol according to [53]**
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 mechanisms

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

1. **PACE Protocol according to [53]**
2. **Authentication Mechanisms based on Triple-DES and AES**

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

1. **PACE Protocol according to [53]**
2. **Passive Authentication according to [43]**
3. **Secure messaging in MAC-ENC mode according to [53]**

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 Personalization Agent by Authentication Mechanism with Personalization Agent Key(s)**

FIA_UAU.6/PACE Re-authenticating

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

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

1. **To establish the communication channel**
2. **Carrying out the PACE Protocol according to [53]**

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.

FMT_MTD.1/PACE_KEY_READ Management of TSF data

FMT_MTD.1.1/PACE_KEY_READ The TSF shall restrict the ability to **read** the

1. **PACE passwords**
2. **Personalization Agent Keys**

to **none**.

FMT_SMF.1 Specification of Management Functions

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

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

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. **Terminal**
2. **PACE authenticated BIS-PACE**
3. **Manufacturer**
4. **Personalization Agent**

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

FPT_EMS.1/PACE TOE Emanation

FPT_EMS.1.1/PACE The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to

1. **PACE: Session Keys (PACE-KMAC, PACE-KENC), Ephemeral Private Key ephem SKPICC-PACE**

FPT_EMS.1.2/PACE The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to

1. **PACE: Session Keys (PACE-KMAC, PACE-KENC), Ephemeral Private Key ephem SKPICC-PACE**

FTP_ITC.1/PACE Inter-TSF trusted channel

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

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

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

FPT_TST.1/PACE TSF testing

FPT_TST.1.1/PACE The TSF shall run a suite of self tests to demonstrate the correct operation of self tests **at the conditions:**

1. **At reset**

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

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

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

FMT_MTD.1/PA Management of TSF data

FMT_MTD.1.1/PA The TSF shall restrict the ability to **write** the **Document Security Objects (SOD)** to **Personalization Agent**.

FMT_MTD.1/INI_ENA Management of TSF data

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

FMT_MTD.1/INI_DIS Management of TSF data

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

FAU_SAS.1 Audit storage

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

8.1.5 PACE CAM SFR

FIA_UAU.1/PACE_CAM Timing of authentication

FIA_UAU.1.1/PACE_CAM The TSF shall allow

1. **Carrying out the PACE Protocol according to [53]**

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

FIA_UAU.1.2/PACE_CAM 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_CAM Single-use authentication mechanisms

FIA_UAU.4.1/PACE_CAM The TSF shall prevent reuse of authentication data related to **Additionally to FIA_UAU.4/PACE**

1. **PACE CAM Protocol according to [53]**

FIA_UAU.5/PACE_CAM Multiple authentication mechanisms

FIA_UAU.5.1/PACE_CAM The TSF shall provide

1. **PACE CAM Protocol according to [53]**

to support user authentication.

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

1. **The same rules from FIA_UAU.5.2/PACE applies, with the PACE_CAM protocol**

FIA_UAU.6/PACE_CAM Re-authenticating

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

FIA_UID.1/PACE_CAM Timing of identification

FIA_UID.1.1/PACE_CAM The TSF shall allow additionally to FIA_UID.1/PACE:

1. **Carrying out the PACE CAM Protocol according to [53]**

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

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

FMT_MTD.1/PACE_CAM_KEY_READ Management of TSF data

FMT_MTD.1.1/PACE_CAM_KEY_READ The TSF shall restrict the ability to **read** the

1. **PACE passwords**
2. **PACE CAM Private Key**

to **none**.

FMT_MTD.1/PACE_CAM_KEY_WRITE Management of TSF data

FMT_MTD.1.1/PACE_CAM_KEY_WRITE The TSF shall restrict the ability to **write** the **PACE CAM private key** to **Personalization Agent**

8.2 Security Assurance Requirements

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

9 TOE Summary Specification

9.1 TOE Summary Specification

Access Control in reading

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

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

1. PACE keys
2. PACE CAM keys
3. Active Authentication private key
4. Personalization Agent keys
5. MSK
6. CVCA keys

It controls access to the CPLC data as well:

1. It ensures the CPLC data can be read during the personalization phase
2. It ensures it cannot be readable in free mode at the end of the personalization step

Regarding the file structure:

In the operational use:

1. The terminal can read user data (except DG3 & DG4), the Document Security Object, EF.CVA, EF.COM only after PACE authentication and through a valid secure channel
2. When the PACE was successfully performed, the terminal can only read the DG3 & DG4 provided the access rights are sufficient through a valid secure channel

In the personalization phase

1. The Personalization Agent can read all the data stored in the TOE after it is authenticated by the TOE (using its authentication keys)

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

Access Control in writing

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

This security functionality ensures the application locks can only be written once in personalization phase to be set to “1”.

It ensures as well the CPLC data cannot be written anymore once the TOE is personalized and that it is not possible to change the personalizer authentication keys in personalization phase.

Regarding the file structure:

In the operational use, it is not possible to create any files (system or data files). Furthermore, it is not possible to update any system files. However:

1. The application data is still accessed internally by the application for its own needs
2. The root CVCA key files and temporary key files are updated internally by the application according to the authentication mechanism described in [43].

In the personalization phase

1. The Personalization Agent can create and write through a valid secure channel all the data files it needs after it is authenticated by the TOE (using its authentication keys)

Active Authentication

This security functionality ensures the Active Authentication is performed as described in [43] (if it is activated by the personalizer).

Chip Authentication

This security functionality ensures the Chip Authentication is performed as described in [43] (if it is activated by the personalizer). It could be used as an alternative of Active Authentication to reinforce the Authentication of the Chip. It differs from an EAC not performing the Terminal Authentication.

PACE mechanism
This security functionality ensures the PACE is correctly performed. It can only be performed once the TOE is personalized with the PACE password. Furthermore, this security functionalities ensures the correct calculation of the PACE session keys.

PACE_CAM mechanism
This security functionality ensures the PACE_CAM is correctly performed. It can only be performed once the TOE is personalized with:
the chip authentication mapping (CAM) keys the Personalization Agent loaded during the personalization phase
1. the PACE password.

Furthermore, this security functionality ensures the correct calculation of the PACE_CAM session keys.

Personalization
This security functionality ensures the TOE, when delivered to the Personalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm. This TSF can use a Secure Messaging described in the TSF Secure Messaging.
This function allow to configure SM level for biometrical data access and the BAC deactivation mechanism

Physical protection
This security functionality protects the TOE against physical attacks.

Pre-personalization
This security functionality ensures the TOE, when delivered to the Pre-personalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm. This function is in charge of pre-initializing the product. This TSF can use a Secure Messaging described in the TSF Secure Messaging.

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

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

Secure Messaging
This security functionality ensures the confidentiality, authenticity & integrity of the channel the TOE and the IFD are using to communicate.
After a successful PACE authentication and successful Chip Authentication, a secure channel is established based on Triple DES algorithm, and after a successful Chip Authentication , a secure channel is (re)established based on Symmetric algorithms (Triple DES, AES128, 192 or 256)
This security functionality ensures:
1. No commands were inserted, modified nor deleted within the data flow
2. The data exchanged remain confidential
3. The issuer of the incoming commands and the destination of the outgoing data is the one that was authenticated (through PACE)

If an error occurs in the secure messaging layer, the session keys are destroyed.
This Secure Messaging can be combined with the Active Authentication.
This TSF can provide a GP Secure Messaging (SCP02 or SCP03) for the Pre-personalization or Personalization.

Self tests
The TOE performs self tests to verify the integrity on the TSF data:

1. At reset.

9.2 Link between the SFR and the TSF

	FCS_CKM.1/DH_PACE	FCS_CKM.4	FCS_COP.1/PACE_ENC	FCS_COP.1/PACE_MAC	FCS_RND.1	FIA_AFL.1/PACE	FIA_UID.1/PACE	FIA_UAU.1/PACE	FIA_UAU.4/PACE	FIA_UAU.5/PACE	FIA_UAU.6/PACE	FDP_ACC.1/TRM	FDP_ACF.1/TRM	FDP_RIP.1	FDP_UCT.1/TRM	FDP_UIT.1/TRM	FTP_ITC.1/PACE	FAU_SAS.1	FMT_SMF.1	FMT_SMR.1/PACE	FMT_LIM.1	FMT_LIM.2	FMT_MTD.1/INI_ENA	FMT_MTD.1/INI_DIS	FMT_MTD.1/KEY_READ	FMT_MTD.1/PA	FPT_EMS.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3
Access Control in reading			x	x		x	x	x	x	x	x	x	x		x	x	x			x				x	x					
Access Control in writing															x	x			x				x			x				
Active Authentication		x			x																						x			
Chip Authentication		x			x																						x			
PACE mechanism	x	x	x	x	x	x	x						x				x										x			
PACE_CAM mechanism		x			x															x							x			
Personalization					x														x	x			x				x			
Physical protection																		x			x	x								x
Pre-personalization					x		x	x	x	x	x								x	x			x				x			
Safe state management																		x	x	x	x	x					x	x		
Secure Messaging	x	x	x	x	x		x	x	x	x	x		x	x			x										x			
Self tests					x																								x	

Table 25: Link between SFR from PP0068v2 and TSF

	FIA_API.1/CA	FCS_CKM.1/CA	FCS_COP.1/CA_SHA	FCS_COP.1/CA_ENC	FCS_COP.1/CA_MAC	FDP_ITC.1/CA	FIA_UAU.1/CA	FIA_UAU.5/CA	FIA_UAU.6/CA	FIA_UID.1/CA	FMT_MTD.1/CA_KEY_WRITE	FMT_MTD.1/CA_KEY_READ	FDP_UCT.1/CA	FDP_UIT.1/CA
Access Control in reading														
Access Control in writing														
Active Authentication														
Chip Authentication	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PACE mechanism														
PACE_CAM mechanism														
Personalization		X												
Physical protection														
Prepersonalization														
Safe state management														
Secure Messaging														
Self tests														

Table 26: Link between Additional SFR for CA and TSF

	FCS_COP.1/AA	FDP_DAU.1/AA	FDP_ITC.1/AA	FMT_MOF.1/AA	FMT_MTD.1/AA_KEY_WRITE	FMT_MTD.1/AA_KEY_READ
Access Control in reading						
Access Control in writing			X			
Active Authentication	X	X	X	X	X	X
Chip Authentication						
PACE mechanism						
PACE_CAM mechanism						
Personalization						
Physical protection						
Prepersonalization						
Safe state management						
Secure Messaging						
Self tests						

Table 27: Link between SFR for AA and TSF

	FIA_UAU.1/PACE_CAM	FIA_UAU.4/PACE_CAM	FIA_UAU.5/PACE_CAM	FIA_UAU.6/PACE_CAM	FIA_UID.1/PACE_CAM	FMT_MTD.1/PACE_CAM_KEY_READ	FMT_MTD.1/PACE_CAM_KEY_WRITE
Access Control in reading	x	x	x	x	x	x	
Access Control in writing							x
Active Authentication							
Chip Authentication							
PACE mechanism							
PACE_CAM mechanism	x	x	x	x	x	x	x
Personalization							
Physical protection							
Prepersonalization					x		
Safe state management							
Secure Messaging	x	x	x		x		
Self tests							

Table 28: Link between Additional SFR for PACE_CAM and TSF

10 Rationales

10.1 Security objectives and Security Problem Definition

10.1.1 Threats

T.Skimming
This threat 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_Int**, **OT.Data_Auth** and **OT.Data_Conf** through the PACE authentication. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the travel document holder itself or by an authorized person or device, and, hence, cannot be captured by an attacker.

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

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

T.Forgery
The threat T.Forgery "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Data_Auth** respectively. The objectives **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" 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.Pass_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE.
Additionally, the examination of the presented eMRTD book according to **OE.Terminal** "Examination of the physical part of the travel document" and **OE.Exam_MRTD_AA** shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

T.Abuse-Func
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.

T.Information_Leakage
The threat T.Information_Leakage "Information Leakage from MRTD's chip" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective **OT.Prot_Inf_Leak**

T.Phys-Tamper

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

T.Malfunction
The threat T.Malfunction "Malfunction due to Environmental Stress" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective **OT.Prot_Malfunction** "Protection against Malfunctions".

T.Counterfeit
The threat T.Counterfeit "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip and identification and authenticity proof required by **OT.CA_Proof** and **OT.Data_Int_CA** using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_MRTD** "MRTD Authentication Key". According to **OE.Terminal** "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.
This attack is also thwarted by Active Authentication proving the authenticity of the chip as required by **OT.AA_Proof** and **OT.Data_Int_AA** using a authentication key pair to be generated by the issuing State or Organization. The Public active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects. **OE.Activ_Auth_Verif** covers also this threat enabling the possibility of performing an Active Authentication which reinforce the security associated to the communication.

10.1.2 Organisational Security Policies

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

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

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

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

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

P.Activ_Auth
The OSP P.Activ_Auth requires the implementation of the Active Authentication protocol as enforced by **OT.AA_Proof**.

P.Chip_Auth

The OSP P.Chip_Auth requires the implementation of the Chip Authentication protocol as enforced by **OT.CA_Proof**.

10.1.3 Assumptions

A.Passive_Auth
This assumption is directly addressed by **OE.Pass_Auth_Sign** requiring the travel document issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on travel document. It therefore covers the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs.

A.Insp_Sys_AA
The examination of the MRTD passport book addressed by the assumption A.Insp_Sys_AA "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD_AA** "Examination of the MRTD passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD_AA** "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Active Authentication Protocol and to protect the logical MRTD data during the transmission and the internal handling.

A.Insp_Sys_CA
The examination of the MRTD passport book addressed by the assumption A.Insp_Sys_CA "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD_CA** "Examination of the MRTD passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD_CA** "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Chip Authentication Protocol and to protect the logical MRTD data during the transmission and the internal handling.

A.Signature_PKI
The assumption is directly covered by the security objective for the TOE environment **OE.Pass_Auth_Sign** “Authentication of logical MRTD by Signature” covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_MRTD_CA** “Examination of the MRTD passport book”. The threat is also covered by **OE.Activ_Auth_Sign** covering the necessary procedures for the Active Authentication key pair establishment.

10.1.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Skimming	OT.Data_Int, OT.Data_Auth, OT.Data_Conf, OT.MRTD_Holder	Section 10.1.1
T.Eavesdropping	OT.Data_Conf	Section 10.1.1
T.Tracing	OT.Tracing, OE.Travel_Document_Holder	Section 10.1.1
T.Forgery	OT.AC_Pers, OE.Personalization, OT.Data_Int, OT.Data_Auth, OT.Prot_Phys-Tamper, OT.Prot_Abuse-Func, OE.Terminal, OE.Pass_Auth_Sign, OE.Exam_MRTD_AA	Section 10.1.1
T.Abuse-Func	OT.Prot_Abuse-Func, OE.Personalization	Section 10.1.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 10.1.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 10.1.1
T.Malfunction	OT.Prot_Malfunction	Section 10.1.1
T.Counterfeit	OT.CA_Proof, OT.Data_Int_CA, OE.Terminal, OT.AA_Proof, OT.Data_Int_AA, OE.Activ_Auth_Verif	Section 10.1.1

Table 29: Threats and Security Objectives - coverage

OSP	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 10.1.2
P.Pre_operational	OT.Identification, OT.AC_Pers, OE.Personalization, OE.Legislative_Compliance	Section 10.1.2
P.Card_PKI	OE.Pass_Auth_Sign	Section 10.1.2

P.Trustworthy_PKI	OE.Pass_Auth_Sign	Section 10.1.2
P.Terminal	OE.Terminal	Section 10.1.2
P.Activ_Auth	OT.AA_Proof	Section 10.1.2
P.Chip_Auth	OT.CA_Proof	Section 10.1.2

Table 30: OSPs and Security Objectives - Coverage

Assumptions	OE	Rationale
A.Passive_Auth	OE.Pass_Auth_Sign , OE.Terminal	Section 10.1.3
A.Insp_Sys_AA	OE.Exam_MRTD_AA, OE.Prot_Logical_MRTD_AA	Section 10.1.3
A.Insp_Sys_CA	OE.Exam_MRTD_CA, OE.Prot_Logical_MRTD_CA	Section 10.1.3
A.Signature_PKI	OE.Pass_Auth_Sign, OE.Exam_MRTD_CA, OE.Activ_Auth_Sign	Section 10.1.3

Table 31: Assumptions and OE - Coverage

10.2 Security requirements and security objectives

10.2.1 Objectives

10.2.1.1 Security Objectives for the TOE

OT.Identification
The security objective OT.Identification "Identification and Authentication of the TOE" addresses the storage of the Initialization and Pre-personalization Data in its non-volatile memory, whereby they also includes 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 Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR **FMT_MTD.1/INI_DIS** allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.

OT.AC_Pers
"Access Control for Personalization of logical travel document" addresses also the access control of the writing the logical travel document. The justification for the SFRs **FAU_SAS.1**, **FMT_MTD.1/INI_ENA** and **FMT_MTD.1/INI_DIS** arises from the justification for OT.Identification above with respect to the Pre-personalization Data.

FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalization data). The SFRs **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 Personalization Agent Keys. The write access to the logical travel document data are defined by the SFR **FIA_UID.1/PACE**, **FIA_UAU.1/PACE**, **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM** in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. The SFRs **FMT_MTD.1/KEY_READ, FMT_MTD.1/CA_KEY_READ** and **FPT_EMS.1** restrict the access to the Personalization Agent Keys and the Chip Authentication Private Key. . The SFR **FMT_MTD.1./PACE_CAM_KEY_READ** restricts the access to the CAM Private Key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR **FIA_UAU.4/PACE** and **FIA_UAU.5/PACE**. If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the **FCS_RND.1** (for the generation of the challenge) and **FCS_COP.1/CA_** (to verify the authentication attempt). The session keys are destroyed according to **FCS_CKM.4** after use.

OT.Data_Int

Integrity of personal data" requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by **FPT_PHP.3**.
Logical manipulation of stored user data is addressed by (**FDP_ACC.1/TRM, FDP_ACF.1/TRM**).

FIA_UAU.4/PACE, **FIA_UAU.5/PACE, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE_CAM** and **FCS_CKM.4** represent some required specific properties of the protocols used.
Unauthorized 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, FIA_UID.1/PACE_CAM**, **FIA_UAU.1/PACE_CAM**) using **FCS_CKM.1/DH_PACE** and possessing the special properties **FIA_UAU.5/PACE**, **FIA_UAU.6/PACE, FIA_UAU.5/PACE_CAM**, **FIA_UAU.6/PACE_CAM**. **FDP_RIP.1** requires erasing the values of session keys.
The **SFR FMT_MTD.1/KEY_READ** and **FMT_MTD.1/PACE_CAM_KEY_READ** restrict the access to the PACE passwords and Chip Authentication Private Key.

Only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (**FDP_ACF.1.2/TRM**, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. **FDP_ACF.1.4/TRM**). **FMT_MTD.1/PA** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy.
The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication. The SFR **FIA_UAU.6/CA** and **FDP_UIT.1/TRM** requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to **FCS_CKM.1/CA** (for the generation of shared secret and for the derivation of the new session keys), and **FCS_COP.1/CA** for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to **FCS_CKM.4** after use.
The SFR **FMT_MTD.1/CA_KEY_WRITE** and **FMT_MTD.1/CA_KEY_READ** requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR **FMT_MTD.1/PACE_CAM_KEY_WRITE** and **FMT_MTD.1/PACE_CAM_KEY_READ** requires that the CAM Key cannot be written unauthorized or read afterwards.

The SFR **FCS_RND.1** represents a general support for cryptographic operations needed.
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 as trustworthy.

OT.Data_Auth
This objective aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC.
A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (**FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UID.1/PACE_CAM, FIA_UAU.1/PACE_CAM**) using **FCS_CKM.1/DH_PACE** resp. **FCS_CKM.1/CA** and possessing the special properties **FIA_UAU.5/PACE**, **FIA_UAU.6/PACE, FIA_UAU.5/PACE_CAM**, **FIA_UAU.6/PACE_CAM** resp. **FDP_RIP.1** requires erasing the values of session keys (here: for K_{MAC}). **FIA_UAU.4/PACE**, **FIA_UAU.5/PACE, FIA_UAU.4/PACE_CAM**, **FIA_UAU.5/PACE_CAM** and **FCS_CKM.4** represent some required specific properties of the protocols used.

The SFR **FMT_MTD.1/CA_KEY_READ** and **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords and the Chip Authentication Private Key.

The SFR **FMT_MTD.1/PACE_CAM_KEY_WRITE** and **FMT_MTD.1/PACE_CAM_KEY_READ** requires that the CAM Key cannot be written unauthorized or read afterwards.

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 as trustworthy. The SFR **FCS_RND.1** represents a general support for cryptographic operations needed. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.
.

OT.Data_Conf
This objective aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (**FDP_ACC.1/TRM**, **FDP_ACF.1/TRM**). **FIA_UAU.4/PACE, FIA_UAU.4/PACE_CAM**, **FIA_UAU.5/PACE, FIA_UAU.5/PACE_CAM** and **FCS_CKM.4** represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by **FDP_UCT.1/TRM**, **FDP_UIT.1/TRM** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_ENC** resp. **FCS_COP.1/CA** A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (**FIA_UID.1/PACE**, **FIA_UAU.1/PACE, FIA_UID.1/PACE_CAM**, **FIA_UAU.1/PACE_CAM**) using **FCS_CKM.1/DH_PACE** resp. **FCS_CKM.1/CA** and possessing the special properties **FIA_UAU.5/PACE**, **FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM** resp. **FIA_UAU.6/CA**. **FDP_RIP.1** requires erasing the values of session keys (here: for Kenc). The SFR **FMT_MTD.1./KEY_READ** restricts the access to the PACE passwords and the Chip Authentication Private Key. **FMT_MTD.1/PA** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the 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.

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

(i) While establishing PACE communication with CAN or MRZ (non-blocking authorization data) - by **FIA_AFL.1/PACE**

(ii) For listening to PACE communication (is of importance for the current PP, since SOD is card-individual) - **FTP_ITC.1/PACE**

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

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

1. Measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by **FPT_EMS.1**
2. Forcing a malfunction of the TOE, which is addressed by **FPT_FLS.1** and **FPT_TST.1**
3. Physical manipulation of the TOE, which is addressed by **FPT_PHP.3**

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

OT.Prot_Malfunction
The security objective OT.Prot_Malfunction "Protection against Malfunctions" is covered by:

1. **FPT_TST.1** which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code

2. **FPT_FLS.1** which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction

OT.AA_Proof
The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by **FMT_MOF.1/AA** and provided by **FDP_DAU.1/AA** proving the identity and authenticity of the TOE. The Active Authentication relies on **FCS_COP.1/AA** and **FCS_RND.1**. It is performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/AA_KEY_WRITE** and **FMT_MTD.1/AA_KEY_READ**.

OT.Data_Int_AA
The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by **FMT_MOF.1/AA** and provided by **FDP_DAU.1/AA, FDP_ITC.1/AA** proving the identity and authenticity of the TOE.

OT.CA_Proof
The security objective OT.CA_Proof "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by **FIA_API.1** proving the identity of the TOE. The Chip Authentication Protocol defined by **FCS_CKM.1/CA** is performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/CA_KEY_WRITE** and **FMT_MTD.1/KEY_READ**. The Chip Authentication Protocol [44] requires additional TSF according to **FCS_CKM.1/CA and FCS_COP.1/CA** (SHA for the derivation of the session keys and **ENC** for the ENC_MAC_Mode secure messaging). The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.

OT.Data_Int_CA
The security objective OT.Data_Int_CA is ensured by the Chip Authentication Protocol that constructs a trusted channel through the following SFR **FIA_UID.1/CA**, **FDP_ITC.1/CA**, **FIA_UAU.1/CA**, **FIA_UAU.5/CA**, **FIA_UAU.6/CA**, **FDP_UCT.1/CA**, **FDP_UIT.1/CA** and **FIA_API.1/CA**.

10.2.2 Rationale tables of Security Objectives and SFRs

SO	SFR	Rationale
OT.Identification	FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_SMF.1, FMT_SMR.1/PACE	Section 10.2.1
OT.AC_Pers	FAU_SAS.1, FCS_CKM.4, FCS_COP.1/CA, FCS_RND.1, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UID.1/PACE, FMT_MTD.1/PACE_CAM_KEY_READ, FMT_MTD.1/CA_KEY_READ,FMT_MTD.1/INI_DIS,FMT_MTD.1/INI_ENA, FMT_MTD.1/KEY_READ, FMT_MTD.1/PA,FMT_SMF.1, FMT_SMR.1/PACE,FPT_EMS.1	Section 10.2.1
OT.Data_Int	FCS_CKM.1/CA, FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/CA, FCS_COP.1/PACE_MAC, FCS_RND.1, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FIA_UAU.1/PACE, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE, FIA_UAU.5/PACE_CAM, FIA_UAU.6/CA, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FIA_UID.1/PACE, FIA_UID.1/PACE_CAM, FMT_MTD.1/CA_KEY_READ, FMT_MTD.1/CA_KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/PA, FMT_MTD.1/PACE_CAM_KEY_READ, FMT_MTD.1/PACE_CAM_KEY_WRITE, FMT_SMF.1, FPT_PHP.3, FTP_ITC.1/PACE	Section 10.2.1
OT.Data_Auth	FCS_CKM.1/CA, FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/PACE_MAC, FCS_RND.1, FDP_RIP.1, FIA_UAU.1/PACE, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE, FIA_UAU.5/PACE_CAM, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FIA_UID.1/PACE, FIA_UID.1/PACE_CAM, FMT_MTD.1/CA_KEY_READ, FMT_MTD.1/KEY_READ, FMT_MTD.1/PA, FMT_MTD.1/PACE_CAM_KEY_READ, FMT_MTD.1/PACE_CAM_KEY_WRITE, FMT_SMF.1, FMT_SMR.1/PACE, FTP_ITC.1/PACE	Section 10.2.1

SO	SFR	Rationale
OT.Data_Conf	FCS_CKM.1/CA, FCS_CKM.1/DH_PACE, FCS_CKM.4, FCS_COP.1/CA, FCS_COP.1/PACE_ENC, FCS_RND.1, FDP_ACC.1/TRM, FDP_RIP.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FIA_UAU.1/PACE, FIA_UAU.1/PACE_CAM, FIA_UAU.4/PACE, FIA_UAU.4/PACE_CAM, FIA_UAU.5/PACE, FIA_UAU.5/PACE_CAM, FIA_UAU.6/CA, FIA_UAU.6/PACE, FIA_UAU.6/PACE_CAM, FIA_UID.1/PACE, FIA_UID.1/PACE_CAM, FMT_MTD.1/KEY_READ, FMT_MTD.1/PA, FMT_SMF.1, FMT_SMR.1/PACE, FTP_ITC.1/PACE,	Section 10.2.1
OT.Tracing	FIA_AFL.1/PACE, FTP_ITC.1/PACE	Section 10.2.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 10.2.1
OT.Prot_Inf_Leak	FPT_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3	Section 10.2.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 10.2.1
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1	Section 10.2.1
OT.AA_Proof	FMT_MOF.1/AA, FDP_DAU.1/AA, FCS_COP.1/AA, FCS_RND.1, FMT_MTD.1/AA_KEY_WRITE, FMT_MTD.1/AA_KEY_READ	Section 10.2.1
OT.Data_Int_AA	FMT_MOF.1/AA, FDP_DAU.1/AA, FDP_ITC.1/AA	Section 10.2.1
OT.CA_Proof	FIA_API.1, FCS_CKM.1/CA, FMT_MTD.1/CA_KEY_WRITE, FMT_MTD.1/KEY_READ, FCS_COP.1/CA, FMT_SMF.1 FMT_SMR.1/PACE	Section 10.2.1
OT.Data_Int_CA	FIA_UID.1/CA, FIA_UAU.1/CA, FIA_UAU.5/CA, FIA_UAU.6/CA, FDP_UCT.1/CA, FDP_UIT.1/CA, FIA_API.1/CA, FDP_ITC.1/CA	Section 10.2.1

Table 32: Security Objectives and SFRs - Coverage

10.3 Dependencies

10.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
PP 0068 v2		
FCS_CKM.1/DH_PACE	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/CA FCS_CKM.1/DH_PACE
FCS_COP.1/PACE_ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_RND.1	No dependencies	
FIA_AFL.1/PACE	(FIA_UAU.1)	FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	
FIA_UAU.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	
FIA_UAU.5/PACE	No dependencies	
FIA_UAU.6/PACE	No dependencies	
FDP_ACC.1/TRM	(FDP_ACF.1)	FDP_ACF.1/TRM
FDP_ACF.1/TRM	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM, see justification
FDP_RIP.1	No dependencies	
FDP_UCT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM see justification
FDP_UIT.1/TRM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/TRM see justification
FAU_SAS.1	No dependencies	
FMT_SMF.1	No dependencies	
FMT_SMR.1/PACE	(FIA_UID.1)	FIA_UID.1/PACE
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FPT_EMS.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FTP_ITC.1/PACE	No dependencies	
AA SFR		
FCS_COP.1/AA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/AA, see justification
FDP_DAU.1/AA	No dependencies	
FDP_ITC.1/AA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1/TRM, see justification
FMT_MOF.1/AA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AA_KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AA_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
PACE CAM		
FIA_UAU.1/PACE_CAM	(FIA_UID.1)	FIA_UID.1/PACE_CAM
FIA_UAU.4/PACE_CAM	No dependencies	
FIA_UAU.5/PACE_CAM	No dependencies	
FIA_UAU.6/PACE_CAM	No dependencies	
FIA_UID.1/PACE_CAM	No dependencies	
FMT_MTD.1/PACE_CAM_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/PACE_CAM_KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
CA SFR		
FCS_CKM.1/CA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/CA
FCS_COP.1/CA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FDP_ITC.1/CA
FDP_ITC.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC. 2/TRM, see justification
FIA_UID.1/CA	No dependencies	
FIA_UAU.1/CA	(FIA_UID.1)	FIA_UID.1/CA
FIA_UAU.5/CA	No dependencies	
FIA_UAU.6/CA	No dependencies	
FIA_API.1/CA	No dependencies	
FDP_UCT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC. 2/TRM, see justification
FDP_UIT.1/CA	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC. 2/TRM, see justification
FMT_MTD.1/CA_KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE
FMT_MTD.1/CA_KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1/PACE

Table 33: SFRs dependencies

10.3.1.1 Rationale for the exclusion of dependencies

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

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/TRM and FDP_UIT.1/TRM is unsupported. The SFR FDP_UCT.1/TRM and FDP_UIT.1/TRM require the use of secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

The dependency FCS_CKM.4 of FCS_COP.1/AA is unsupported. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4.

The dependency FTP_ITC.1 of FDP_UCT.1/CA and FDP_UIT.1/CA is unsupported. There is no need for FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

10.3.2 SARs dependencies

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

Table 34: SARs dependencies

10.4 EAL rationale

This Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.
EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.
The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

10.5 EAL augmentations rationale

10.5.1 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL5 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.
ALC_DVS.2 has no dependencies.

10.5.2 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.
Advanced methodical vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication. AVA_VAN.5 has dependencies with ADV_ARC.1 "Security architecture description", ADV_FSP.4 "Complete functional specification", ADV_IMP.1 "Implementation representation of the TSF", ADV_TDS.3 "Basic modular design", AGD_PRE.1 "Preparative procedures" and AGD_OPE.1 "Operational user Guidance" and ATE_DPT.1 "Testing: basic design".

All these dependencies are satisfied by EAL5.

11 Acronyms

AA	Active Authentication
BAC	Basic Access Control
CC	Common Criteria Version 3.1 revision 4
CPLC	Card personalization life cycle
DF	Dedicated File
DFA	Differential Fault Analysis
DG	Data Group
EAL	Evaluation Assurance Level
EF	Elementary File
EFID	File Identifier
DES	Digital encryption standard
DH	Diffie Hellmann
I/0	Input/Output
IC	Integrated Circuit
ICAO	International Civil Aviation organization
ICC	Integrated Circuit Card
IFD	Interface device
LDS	Logical Data structure
MF	Master File
MRTD	Machine readable Travel Document
MRZ	Machine readable Zone
MSK	Manufacturer Secret Key
OCR	Optical Character Recognition
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
SFI	Short File identifier
SHA	Secure hashing Algorithm
SOD	Security object Data
TOE	Target of Evaluation
TSF	TOE Security function

Index