ePass ICAO essential

ST lite – EAC RSA

FQR No: 110 7563

FQR Issue: 1

Legal Notice

*** Printed versions of this document are uncontrolled ***

Document Management

A. Identification

Business Unit - Department	ID R&D
Document type:	FQR
Document Title:	ePass ICAO essential - ST lite - EAC RSA
FQR No:	110 7563
FQR Issue:	1

Table of contents

List of Figures

List of tables

1 SECURITY TARGET INTRODUCTION

1.1 Purpose

The objective of this document is to present the Security Target Lite of the ePass ICAO essential product configuration EAC RSA on SLE77.

1.2 Product description

This product is designed to host configurable applications that can satisfy the following use case:

Machine Readable Travel Document.

This present Security Target considers EAC PP [R10].

This product involves the following cryptographic features:

- RSA 1024 to 2048 bits (256 bits steps)
- 3DES (2keys)
- SHA 1, SHA 224, 256
- RNG
- Secure messaging DES
- GP Secure messaging during personalization (SCP02)

The following interfaces are supported:

- Contactless
- Contact

A personalization application is embedded, supporting ISO 7816-4 and proprietary commands.

1.3 Objective of the Security Target

This security target describes the security needs for ePass ICAO essential configuration EAC RSA product. The configuration is conforming to PP BAC and adds requirements for Active Authentication and for Prepersonalization and personalization.

This Security Target aims to satisfy the requirements of Common Criteria level EAL4 augmented ALC_DVS.2 in defining the security enforcing functions of the Target Of Evaluation and describing the environment in which it operates.

The objectives of this Security Target are:

To describe the Target of Evaluation (TOE), its life cycle and to position it in the smart card life cycle.

To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases.

To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the product active phases.

To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment.

To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements.

To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

1.4 Security Target Identification

Title:	Ariane - ST - EAC RSA
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL4 augmented with: AVA_VAN.5 and ALC_DVS.2
PP(s):	E- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009
ST Reference	FQR: 110 7404 Issue 1
ITSEF:	UL
Certification Body:	CESG
Evaluation scheme:	UK

Table 1 - General Identification

1.5 TOE Technical Identification

Product name:	ePass ICAO essential Config BAC + EAC RSA on SLE77
Commercial name for On Infineon SLE77CLFX2400P & SLE77CLFX2407P:	ePass ICAO essential EAC RSA on SLE77

Table 2 - TOE Technical Identification

1.6 IC Identification

IC Reference:	Infineon chips
IC EAL	EAL5+, ALC_DVS.2, AVA_VAN.5
Communication protocol:	Contact, Contactless and Dual
Memory:	Flash
Chip Manufacturer:	Infineon
IC PP	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
IC certificate	BSI-DSZ-CC-0917-2014
IC maintenance	BSI-DSZ-CC-0917-2014-MA-01
IC ST lite	Security Target Lite of M7794 A12 and G12, Version 2.3, 2013-11-27, Infineon Technologies AG.

Table 3 - Chip Identification

1.7 Reference documents

MRTD specifications

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

[R2] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[R3] ICAO Doc 9303, Machine Readable Travel Documents, part 3 – Machine Readable Offical Travel Documents, Specifications for electronically enabled offical travel documents with biometric identification capabilities (including supplement), ICAO doc 93003, 2008

[R4] 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

[R5] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v2.10 part 1

[R6] Annex to Section III Security Standards for Machine Readable Travel Documents Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

Oberthur Technologies Specification

[R7] FQR 110 7226 Ed 1 - ePass ICAO essential - Perso Guide, Oberthur Technologies

Protection Profiles

[R8] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0035 15/06/2007

[R9] Machine readable travel documents with "ICAO Application", Basic Access control – BSI-PP-0055 v1.10 25th march 2009

[R10] E- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009

[R11] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007

[R12] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009

Chips References

[R13] BSI-DSZ-CC-0917 Certification report – SLE77CLFX2400P and SLE77CLFX2407P

[R14] Maintenance report BSI-DSZ-CC-0917 MA01 – SLE77CLFX2400P and SLE77CLFX2407P

Standards

[R15] ISO/IEC 7816-4:2013 – Organization, security and commands for interchange

[R16] Technical Guideline: Elliptic Curve Cryptography according to ISO/IEC 15946.TR-ECC, BSI 2006

[R17] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[R18] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[R19] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[R20] ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[R21] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[R22] Federal Information Processing Standards Publication 180-2 Secure Hash Standard (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[R23] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[R24] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. RFC 3447, 2003

[R25] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002

[R26] ANSI X9.31 - Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[R27] FIPS 46-3 Data Encryption Standard (DES)

[R28] ISO/IEC 9797-1:1999 "Codes d'authentification de message (MAC) Partie 1: Mécanismes utilisant un cryptogramme bloc"

[R29] NIST SP 800-90 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)

[R30] FIPS 197 – Advance Encryption Standard (AES)

[R31] ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996

Misc

[R32] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R33] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

[R34] Advanced Security Mechanisms for Machine Readable Travel Documents part 1 – Technical Guideline TR-03110-1 – version 2.10 March 2012

[R35] Advanced Security Mechanisms for Machine Readable Travel Documents part 2 – Technical Guideline TR-03110-2 – version 2.10 March 2012

[R36] Advanced Security Mechanisms for Machine Readable Travel Documents part 3 – Technical Guideline TR-03110-3 – version 2.10 March 2012

CC

[R37] Common Criteria for Information Technology security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 Revision 4 Final, September 2012

[R38] Common Criteria for Information Technology security Evaluation Part 2: Security Functional Components, CCMB-2012-09-002, version 3.1 Revision 4 Final, September 2012

[R39] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Components, CCMB-2012-09-003, version 3.1 Revision 4 Final, September 2012

2 TOE OVERVIEW

2.1 Product overview

The product **EPass ICAO essential on SLE77** is multi-applicative native software, 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 **Prepersonalization/personalization phases** of the product. For more information on the product, please refer to complete ST.

The product supports the storage and retrieval of structured information compliant to the Logical Data Structure as specified in [R2].

This product is embedded on an IC. The IC functionalities are described §1.6.

2.2 TOE overview

The TOE described in this security target is the BAC with EAC RSA configuration of the product.

The BAC TOE is instantiated during the product prepersonalization, using the Application Creation Engine that creates the MF / DF required for the BAC configuration.

The TOE life cycle is described in **§ 4 TOE life cycle.**

2.3 TOE Usages

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 authorised 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 or any other form factor.

A separate data summary for visual and machine reading using OCR methods in the Machine Readable Zone,

And data elements stored on the TOE's chip for contact and 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.

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 or any other form factor.

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 on the 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 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.

2.4 TOE Definition

The Target of Evaluation (TOE) is the integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to ICAO Doc 9303 and Extended Access Control according to TR 03110.

The physical scope of the TOE is:

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

IC Dedicated Software

IC Embedded Software (operating system)

MRTD application

Associated guidance documentation

2.5 TOE Guidance

The table below identifies the guidance for the personalization of the TOE (the guidance is identical for both TOEs).

Guidance document for Prepersonalization and Personalization	[R7] FQR 110 7226 - ePass ICAO essential - Perso Guide, Oberthur Technologies
Guidance documents for Operational Phase	[R1] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization [R2] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization [R3] ICAO Doc 9303, Machine Readable Travel Documents, part 3 – Machine Readable Offical Travel Documents, Specifications for electronically enabled offical travel documents with biometric identification capabilities (including supplement), ICAO doc 93003, 2008 [R34] Advanced Security Mechanisms for Machine Readable Travel Documents part 1 – Technical Guideline TR-03110-1 – version 2.10 March 2012 [R36] Advanced Security Mechanisms for Machine Readable Travel Documents part 3 – Technical Guideline TR-03110-3 – version 2.10 March 2012

Table 4: TOE Guidance reference

2.6 TOE identification

The means to identify the TOE is presented in the chapter 3 of guidance for personalization [R7].

3 TOE ARCHITECTURE

The TOE is an IC with software, composed of various modules and composed of the following components:

The **EPass ICAO essential configuration BAC + EAC RSA on SLE77** architecture can be viewed as shown in the following picture:

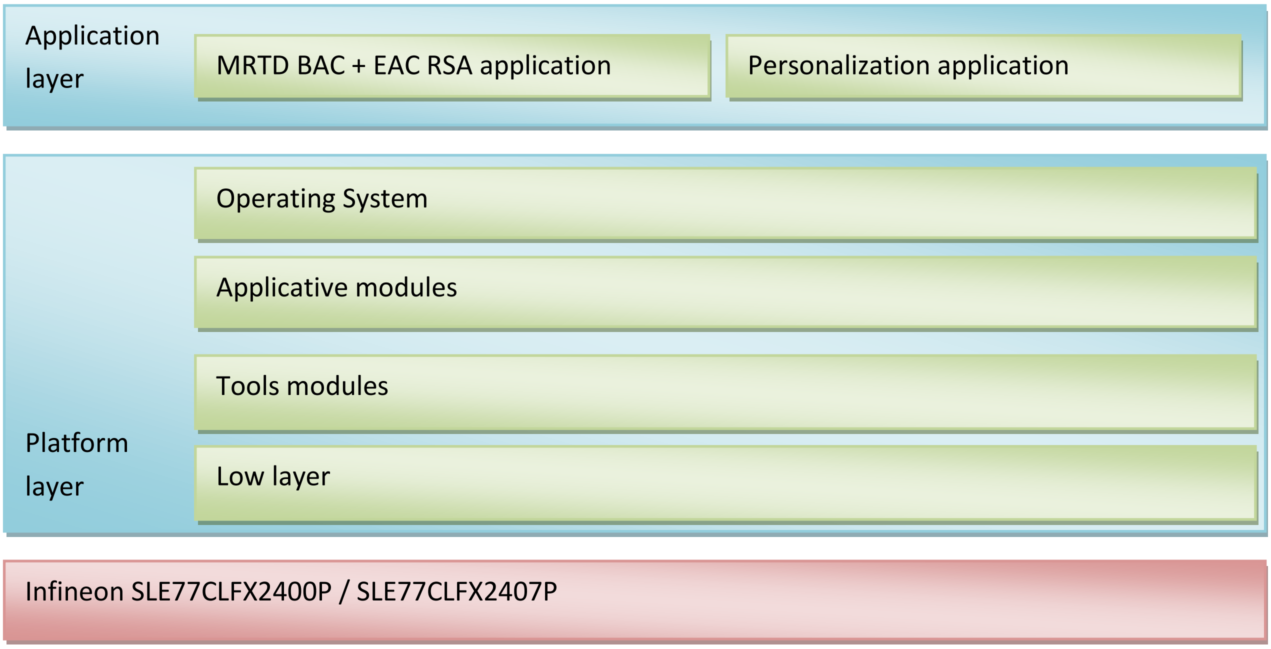
Application layer
MRTD BAC + EAC RSA application
Personalization application
Operating System
Applicative modules
Tools modules
Platform layer
Low layer
Infineon SLE77CLFX2400P / SLE77CLFX2407P

Figure 1 - TOE architecture

3.1 Integrated Circuit – Infineon SLE 77

The TOE is embedded on Infineon chips, as presented in **Table 3 - Chip Identification.**
The IC part of the TOE comprises the following:

Core System:

CPU
Memory Encryption/Decryption Unit (MED)
Memory Management Unit (MMU)

Memories:

Read-Only Memory (ROM)
Random Access Memory (RAM)
SOLID FLASH™ NVM

Peripherals:

- True Random Number Generator (TRNG)
- Pseudo Random Number Generator (PRNG)
- Watchdog and timers
- Universal Asynchronous Receiver/Transmitter (UART)
- Checksum module (CRC)
- Radio Frequency Interface (RFI)

Control:

- Dynamic Power Management
- Internal Clock Oscillator (ICO)
- Interrupt and Peripheral Event Channel Controller (ITP and PEC)
- Interface Management Module (IMM)
- User mode Security Life Control (UmSLC)
- Voltage regulator

Coprocessors:

- Crypto2304T for asymmetric algorithms like RSA and EC
- Symmetric Crypto Coprocessor for AES and 3DES Standard

Security Peripherals:

- Filters
- Sensors

Buses:

- Memory Bus
- Peripheral Bus

And associated Firware and Sofware, it comprises:
RMS and SAM routines for Solid Flash NVM programming; security functions test, random number online testing. STS consisting of test and initialization routines. All stored in the ROM part.
The Flash Loader that allows the loading of TOE software.
And cryptographic libraries.

IC is part of the TOE and also part of the TSF. More information on the chips is given in the related Security Target.

3.2 Low layer

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

The main features of the OS are the following:
Management Memories and secure data processing,
Transaction management,
APDU protocol management,
Low level T=0 ; T=1 and T=CL management (type A and type B),
Error processing.

A dedicated cryptographic library has been developed and designed by Oberthur Technologies to provide the highest security level and best tuned performances. It provides the following algorithms:

Cryptographic Feature	Embedded
SHA1, SHA-224, SHA-256	✓
RSA from 1024, to 2048 bits (by steps of 256 bits) - verification (for EAC) - key agreement DH (for session keys)	✓
3DES with 112 bits key size	✓
Random Generator compliant AIS31	✓

Table 5 - Supported Cryptography

More information is available in complete ST.
Low layer is part of the TOE and is also part of the TSF.

3.3 Tools modules

The tools modules provide ePAss ICAO essential product:

- File system compliant with ISO/IEC 7816-4 and ISO/IEC 7816-9. It is also compliant with ICAO recommendations[R1].
- ISO Secure Messaging as specified in [R15] and as described in annex E of [R36].
- Asymmetric Keys Management as storage, signature, verification, DH and generation.
- Symmetric Key management
- Access Control for ‘Change MSK’ and ‘PUT KEY’ APDU
- Authentication and secure messaging to be used during Prepersonalization and Personalization phases, based on Global Platform standard

More information is available in complete ST.

Tools modules are part of the TOE and are also part of the TSF.

3.4 Applicative modules

The applicative modules provide ePass ICAO essential product:

- Chip Authentication used to authenticate the card to the terminal. This authentication service is made available to the MRTD application.
- Terminal Authentication used to authenticate the terminal to the card. This authentication service is made available to the MRTD application.
- Access Conditions Engine that checks the AC rules attached to an object (file, key, data object) with a current context (CHA, Role ID…).

More information is available in complete ST.
Those applicative modules are part of the TOE and are also part of the TSF.

Another applicative module is the Digital Blurred Image (DBI) module. It allows the blurring of a JPG or JPEG2000 file stored in a transparent file. This feature is the implementation of patents owned by Oberthur Technologies. More information is available in complete ST.

This module is part of the TOE and outside the scope of this present certification.

3.5 Operating System

The operating system manages the TOE in pre-personalization and personalization phases in order to configure the TOE in the expected way. It implements and control access to Key management (MSK) or File management including data reading and writing. It can be addressed in clear mode for secure environment or non-sensitive commands or using SCP02.

The operating system also manages protocols available during Use phase such as Basic Access Control or Active Authentication. The protocol for Basic Access Control is specified by ICAO [R2]. 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 [R31] 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 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.

More information is available in complete ST.
The Operating System is part of the TOE and is also part of the TSF.

3.6 Application layer

Two kinds of applications are available on the top of the product: MRTD EAC RSA and resident application used for Personalization.

More information is available in complete ST.
This layer is part of the TOE and is also part of the TSF.

4 TOE LIFE CYCLE

4.1 Life cycle overview

The TOE life-cycle is described in terms of four life-cycle phases. (With respect to the [R8], the TOE life-cycle is additionally subdivided into 7 steps). The table below presents the TOE role:

Roles	Subject
IC developer	Infineon
IC manufacturer	Infineon
Embedded software developer	Oberthur Technologies
Module Manufacturer	Oberthur Technologies or Infineon
Prepersonalizer	Oberthur Technologies or another agent: Agent in charge of the Prepersonalization This additional subject is a refinement of the role Manufacturer as described in [R9]. It is the agent in charge of the Prepersonalization of the TOE. It corresponds to the MRTD manufacturer as described in [R9]
Personalization Agent	The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the DSO.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Table 6 - 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 [R8], the TOE delivery point and the coverage:

Steps	Phase	Subject	Covered by
Step 1	Development	Oberthur Technologies	ALC R&D sites

	(Phase1)		
Step 2	Development (Phase1)	Infineon	IC certification
Step 3	Manufacturing (Phase2)	Infineon (code loading in flash Memory)	IC certification
Step 4	Manufacturing (Phase2)	Oberthur Technologies Manufacturer (Code loading in flash Memory)	ALC sites
TOE delivery point			
Step 5	Manufacturing (Phase2)	Prepersonalization or Other agent	AGD_OPE & AGD_PRE
Step 6	Personalization (p	Oberthur Technologies Personalization or Other agent	AGD_OPE & AGD_PRE
Step 7	Operational Use	End user	AGD_OPE & AGD_PRE

Table 7 - Subjects identification following life cycle steps

The figure below summarizes the different phases of the development of any configuration of the ePass ICAO Essential family.

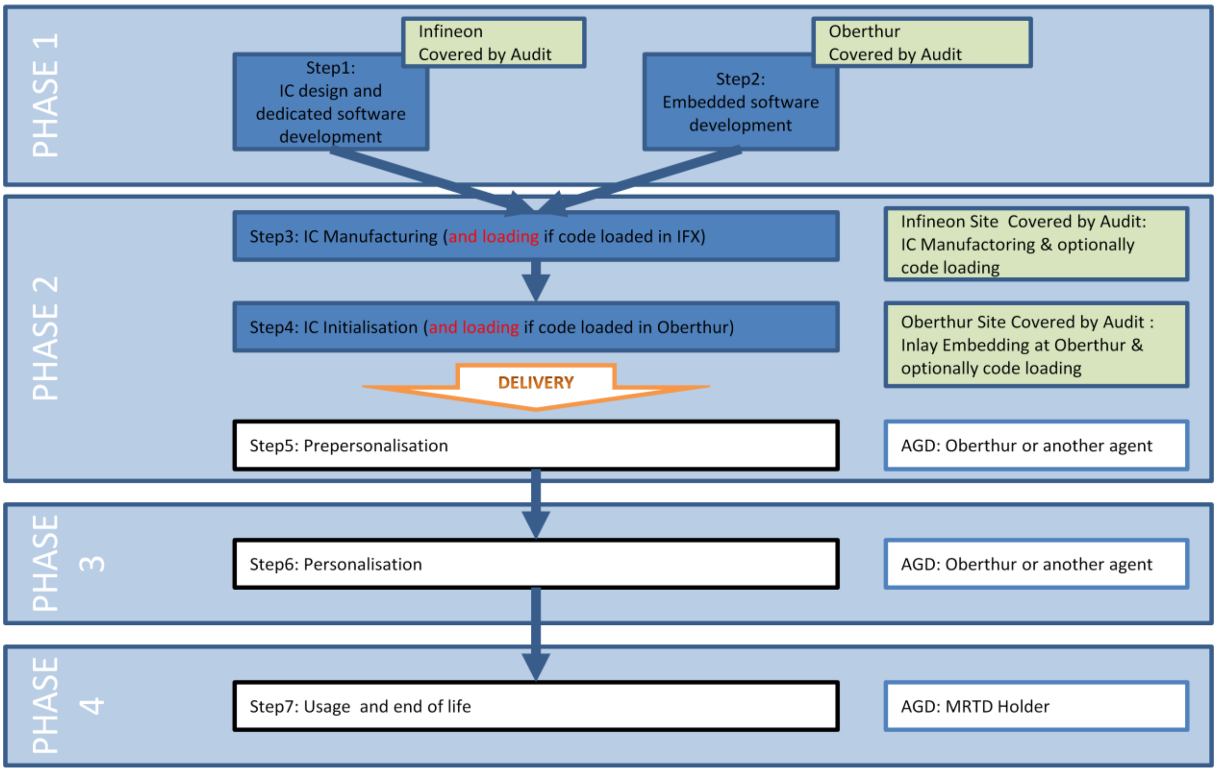
PHASE 1
Infineon
Covered by Audit
Step1:
IC design and
dedicated software
development
Oberthur
Covered by Audit
Step2:
Embedded software
development
PHASE 2
Step3: IC Manufacturing (and loading if code loaded in IFX)
Infineon Site Covered by Audit:
IC Manufactoring & optionally
code loading
Step4: IC Initialisation (and loading if code loaded in Oberthur)
Oberthur Site Covered by Audit :
Inlay Embedding at Oberthur &
optionally code loading
DELIVERY
Step5: Prepersonalisation
AGD: Oberthur or another agent
PHASE 3
Step6: Personalisation
AGD: Oberthur or another agent
PHASE 4
Step7: Usage and end of life
AGD: MRTD Holder

Figure 2: ePass ICAO Essential life cycle

4.2 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.

(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 Oberthur Technologies Code with associated documentation is ready to be loaded in the flash memory.

4.3 Phase 2 “Manufacturing”

(Step 3) The Oberthur Technologies code is loaded in the flash memory, this operation can be done in the step 3 and in the step 4:

At Infineon site; the code is then securely delivered to the IC manufacturer. The Infineon site is covered by an audit, step 3.

Or at Oberthur Technologies manufacturing Site. The code is then securely transferred to audited Oberthur Technologies factories, step 4.

(Step) When the code is loaded by Infineon in the Step 3, the TOE integrated circuit is produced containing the travel document’s chip Dedicated Software in the flash memories. The 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 manufacturer adds initialization data and keys. The product is self protected, security functions are active. The product can be sent:

to Oberthur Technologies or

directly to Oberthur Technologies Customers.

(Step4) Oberthur Technologies load the Code and data on the flash memories. The IC contains the MRTD code and data with the required protection. The product can be sent to Oberthur Technologies customers (another agent).

TOE delivery point

(Step5) The Manufacturer (i) adds the IC Embedded Software or part of it, (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.

4.4 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,

the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits),

the personalization of the visual readable data onto the physical part of the travel document,

the writing of the TOE User Data and TSF Data into the logical travel document and

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 objects. 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.

4.5 Phase 4 “Operational Use”

(Step7) The TOE is used as a travel document's chip by the traveler 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 outlines 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.

5 CONFORMANCE CLAIMS

5.1 Common Criteria conformance

This Security Target (ST) claims conformance to the Common Criteria version 3.1 revision 4 [R37], [R38] and [R39].

The conformance to the CC is claimed as follows:

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

Table 8 - Conformance Rationale

Remark:

For interoperability reasons it is assumed the receiving state cares for sufficient measures against eavesdropping within the operating environment of the inspection systems. Otherwise the TOE may protect the confidentiality of some less sensitive assets (e.g. the personal data of the TOE holder which are also printed on the physical TOE) for some specific attacks only against enhanced basic attack potential (AVA_VAN.3).

FPT_EMSEC.1 from the Protection Profile has been renamed to FPT_EMS.1, in order to keep the SFR formatting.

5.2 Protection Profile conformance

5.2.1 Protection Profile claims

The Security Target claims strict conformance to the following PPs written in CC3.1 revision 2:

[R10] E- Machine readable travel documents with “ICAO Application”, Extended Access control – BSI-PP-0056 v1.10 25th march 2009.

6 SECURITY PROBLEM DEFINITION

6.1 Subjects

SFR	Before phase 2	Phase 2	Phase 3	Phase 4
PP EAC subjects				
Manufacturer	x	x		
Personalization Agent			x	
Terminal		x	x	x
Inspection System				x
MRTD Holder				x
Traveler				x
Attacker	x	x	x	x
Additional subjects				
IC Developer	x			
Software Developer	x			
Prepersonalizer (refinement of Manufacturer. It corresponds to the MRTD manufacturer)		x		

Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [R2].

Application Note:

Personalization Agent is referred as the Personalizer in the Security Target.

Country Verifying Certification Authority

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

Document Verifier

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

Terminal

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

Inspection System (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless communication with the MRTD’s chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Attacker

A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Application Note

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

Additional Subjects

IC Developer

Developer of the IC.

TOE Developer

Developer of part of the TOE source code.

Prepersonalizer

Agent in charge of the Prepersonalization. This agent corresponds to the MRTD manufacturer as described in [R9].

6.2 Assets

Logical MRTD data

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

Application note:

Due to interoperability reasons the 'ICAO Doc 9303' requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. Note the BAC mechanisms may not resist attacks with high attack potential.

""The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [R2]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (CAPK) in EF.DG 14 is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.""

User Data	Description
CPLC Data	Data uniquely identifying the chip. They are considered as user data as they enable to track the holder

User Data	Description
Personal Data of the MRTD holder (EF.DGx, except EF.DG15)	Contains identification data of the holder
Document Security Object (SOD) in EF.SOD	Contain a corticated ensuring the integrity of the file stored within the MRTD and their authenticity. It ensures the data are issued by a genuine country
Common data in EF.COM	Declare the data the travel document contains. This data is optional and may be absent in the TOE

Table 9 - User Data

TSF Data	Description
TOE_ID	Data enabling to identify the TOE
Prepersonalizer reference authentication data	Private key enabling to authenticate the Prepersonalizer
Personalization Agent reference authentication Data	Private key enabling to authenticate the Personalization Agent
Basic Access Control (BAC) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Chip Authentication Private key (CAK)	Private key used by the Chip to perform a Chip Authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality, authenticity and integrity
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 10 - TSF Data

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

6.3 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.

Application note: The threats T.Chip_ID and T.Skimming (cf [R27]) are averted by the mechanisms described in the BAC PP which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD’s chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

Next threats presented are all related to and issued from PP EAC.

T.Read_Sensitive_Data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [R10]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

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

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

T.Forgery

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder’s identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another

MRTD’s chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

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

Asset: authenticity of logical MRTD data.

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 traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

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

Asset: authenticity of logical MRTD data

T.Abuse-Func

Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality of logical MRTD and TSF data.

T.Phys-Tamper

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.

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

Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

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 or (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 enhanced basic attack potential, being in possession of a legitimate MRTD.

Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.TOE_Identification_Forgery

Adverse action: An attacker tries to perturbate the TOE identification.

Threat agent: having high attack potential, being in possession of a legitimate MRTD

Asset: TOE_ID

6.4 Organisational Security Policies

P.BAC-PP

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the "ICAO Doc 9303" [R2] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [R9] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

Application note: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [R2] is addressed by the [R9] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [R9]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates.

P.Sensitive_Data

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

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.Personalization

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

6.5 Assumptions

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

A.MRTD_Manufact

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication v1 Public Key (EF.DG14) if stored on the MRTD’s chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD’s chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection

System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

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.

A.Auth_PKI

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

7 SECURITY OBJECTIVES

7.1 Security Objectives for the TOE

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

OT.AC_Pers

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R2] 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. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

OT.Data_Int

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 data.

OT.Sens_Data_Conf

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

OT.Identification

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s). The storage of the Prepersonalization data includes writing of the Personalization Agent Key(s).

OT.Chip_Auth_Proof

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication v1 as defined in [R34]. The authenticity proof provided by the MRTD's chip shall be protected against attacks with high attack potential.

OT.Prot_Abuse-Func

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to:

- (i) Disclose critical User Data
- (ii) Manipulate critical User Data of the IC Embedded Software
- (iii) Manipulate Soft-coded IC Embedded Software
- (iv) Bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip:

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

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. This includes protection against attacks with enhanced-basic attack potential by means of

- Measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- Measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- Manipulation of the hardware and its security features, as well as
- Controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

OT.Prot_Malfunction

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

7.2 Security objectives for the Operational Environment

Issuing State or Organization

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

OE.MRTD_Manufact

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_ Delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- Non-disclosure of any security relevant information
- Identification of the element under delivery
- Meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment)
- Physical protection to prevent external damage
- Secure storage and handling procedures (including rejected TOE"s)
- Traceability of TOE during delivery including the following parameters:
    - Origin and shipment details
    - Reception, reception acknowledgement
    - Location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, and reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

OE.Personalization

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization:

- (i) Establish the correct identity of the holder and create biographical data for the MRTD
- (ii) Enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s)

- (iii) Personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign

The issuing State or Organization must:

- (i) Generate a cryptographic secure Country Signing CA Key Pair
- (ii) Ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment
- (iii) Distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must:

- (i) Generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys
- (ii) Sign Document Security Objects of genuine MRTD in a secure operational environment only
- (iii) Distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [R2].

OE.Auth_Key_MRTD

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

- (i) Generate the MRTD's Chip Authentication Key Pair
- (ii) Sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14
- (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 Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data

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

OE.BAC-PP

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [R9]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

Receiving State or Organization

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

OE.Exam_MRTD

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability:

- (i) Includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization
- (ii) Implements the terminal part of the Basic Access Control [R2]

OE.Passive_Auth_Verif

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD

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

Application note:

The figure 2.1 in [R10] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication Protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this ST. However, the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems

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

8 EXTENDED REQUIREMENTS

8.1 Extended family FAU_SAS - Audit data storage

8.1.1 Extended components FAU_SAS.1

Description: see [R9].

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 [R9]

8.2 Extended family FCS_RND - Generation of random numbers

8.2.1 Extended component FCS_RND.1

Description: see [R9]

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 [R9]

Extended family FIA_API – Authentication proof of identity

Extended component FIA_API.1

Description: see [R10]

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 [R10]

8.3 Extended family FMT_LIM - Limited capabilities and availability

8.3.1 Extended component FMT_LIM.1

Description: See [R9]

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 [R9]

8.3.2 Extended component FMT_LIM.2

Description: See [R9]

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 [R9]

8.4 Extended family FPT_EMS - TOE Emanation

8.4.1 Extended component FPT_EMS.1

Description: See [R9]

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 [R9]

9 SECURITY REQUIREMENTS

9.1 Convention

The following table 'PP SFRs versus ST SFRs' expresses the links between SFRs form PP EAC and SFRs used in the ST (and in the specifications of the TOE). It allows ease evaluation of the ST and ease comparison with the PP EAC.

The first column presents the sfrs with PP extension and the others columns present the same SFRs with extra extensions.

This table presents also the "use" phase of each SFR.

For example, FAU_SAS.1 listed in the column 1 is from the PP EAC. The SFR is specified in this ST as FAU_SAS.1.1/MP and is implemented only in phases 2 and 3, not in phase 4 (MP means in steps Prepersonalization and personalization).

For SFR in Column generic, it means that this sfr is used in all phases (2, 3 and 4) as for example FCS_RND.1.

CA: Chip authentication, TA: Terminal Authentication and EAC: means that the sfr is not specified to TA neither to CA.

These details are useful for the read of functional specification as the TOE FSP uses detailed extension. For coherency with the PP EAC, the present ST for rationales uses the first columns.

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4
SFR from PP EAC			
FAU_SAS.1		FAU_SAS.1.1/MP	
FCS_CKM.1			FCS_CKM.1.1/CA_DH_SM_DES
FCS_CKM.4	FCS_CKM.4.1		
FCS_COP.1/SHA			FCS_COP.1.1/CA_SHA_SM_3DES FCS_COP.1.1/TA_SHA_RSA
FCS_COP.1/SYM			FCS_COP.1.1/CA_SYM_SM_3DES
FCS_COP.1/MAC			

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4
FCS_COP.1/SIG_VER			FCS_COP.1.1/CA_MAC_SM_3DES FCS_COP.1.1/TA_SIG_VER_RSA
FCS_RND.1	FCS_RND.1.1		
FIA_UID.1			FIA_UID.1.1/CA FIA_UID.1.2/CA
FIA_UAU.1			FIA_UAU.1.1/CA FIA_UAU.1.2/CA
FIA_UAU.4		FIA_UAU.4.1/MP_3DES	FIA_UAU.4.1/TA
FIA_UAU.5			FIA_UAU.5.1/CA_3DES FIA_UAU.5.2/CA_3DES FIA_UAU.5.1/EAC FIA_UAU.5.2/EAC FIA_UAU.5.1/MP_3DES FIA_UAU.5.2/MP_3DES
FIA_UAU.6			FIA_UAU.6.1/CA
FIA_API.1			FIA_API.1.1/CA
FDP_ACC.1			FDP_ACC.1.1/EAC
FDP_ACF.1			FDP_ACF.1.1/EAC FDP_ACF.1.2/EAC FDP_ACF.1.3/EAC FDP_ACF.1.4/EAC
FDP_UCT.1			FDP_UCT.1.1/CA
FDP_UIT.1			FDP_UIT.1.1/CA FDP_UIT.1.2/CA
FMT_SMF.1		FMT_SMF.1.1/MP	
FMT_SMR.1		FMT_SMR.1.1/MP FMT_SMR.1.2/MP	FMT_SMR.1.1/TA FMT_SMR.1.2/TA
FMT_LIM.1	FMT_LIM.1.1		FMT_LIM.1.1/EAC
FMT_LIM.2	FMT_LIM.2.1		FMT_LIM.2.1/EAC
FMT_MTD.1/INI_ENA		FMT_MTD.1.1/MP_INI_ENA	
FMT_MTD.1/INI_DIS		FMT_MTD.1.1/MP_INI_DIS	

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4
FMT_MTD.1/CVCA_INI			FMT_MTD.1.1/TA_CVCA_INI
FMT_MTD.1/CVCA_UPD			FMT_MTD.1.1/TA_CVCA_UPD
FMT_MTD.1/CVCA_DATE			FMT_MTD.1.1/TA_CVCA_DATE
FMT_MTD.1/KEY_WRITE			FMT_MTD.1.1/BAC_KEY_WRITE
FMT_MTD.1/CAPK			FMT_MTD.1.1/CAPK
FMT_MTD.1/KEY_READ		FMT_MTD.1.1/MP_KEY_READ	FMT_MTD.1.1/BAC_KEY_READ FMT_MTD.1.1/CA_KEY_READ
FMT_MTD.3			FMT_MTD.3.1/EAC
FPT_EMS.1	FPT_EMS.1.1 FPT_EMS.1.2	FPT_EMS.1.1/MP FPT_EMS.1.2/MP	FPT_EMS.1.1/CA FPT_EMS.1.2/CA
FPT_FLS.1	FPT_FLS.1.1		
FPT_TST.1	FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3		FPT_TST.1.1/CA FPT_TST.1.2/CA FPT_TST.1.3/CA FPT_TST.1.1/TA FPT_TST.1.2/TA FPT_TST.1.3/TA
FPT_PHP.3	FPT_PHP.3		

Table 11: PP EAC SFRs versus ST SFRs details

9.2 Security Functional Requirements issued from the PP EAC

FAU_SAS.1 Audit storage

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

FCS_CKM.1 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 **DH compliant to** PKCS#3 and specified cryptographic key sizes **112bits** that meet the following: [R34][R21], Annex A.1.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1 Cryptographic operation

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

Iteration	**Operation**	**Algo**	**Key Length (bits)**	**Standard**
FCS_COP.1/SHA				
FCS_COP.1.1/CA_SHA_SM_3DES	Hashing	SHA-1	None	FIPS 140-2
FCS_COP.1.1/TA_SHA_RSA	Hashing	SHA-1, SHA-224, SHA-256	None	FIPS 140-2
FCS_COP.1/SYM				
FCS_COP.1.1/CA_SYM_SM_3DES	Encryption and decryption	TDES CBC mode	112	TR-03110 [R34]
FCS_COP.1/MAC				
FCS_COP.1.1/CA_MAC_SM_3DES	Authentication SM MAC	TDERS Retail MAC	112	TR-03110 [R34]
FCS_COP.1/SIG_VER				
FCS_COP.1.1/TA_SIG_VER_RSA	Digital Signature verification	RSA coupled with SHA	From 1024 up to 2048 (by step of 256 bits)	TR-03110 [R34]

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **(1) the requirement to provide an entropy of at least 7.976 bits in each byte, following AIS 31 [R32].**

FIA Identification and Authentication

FIA_UID.1 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 disabled by the TSF according to FMT_MTD.1/INI_DIS

3. To carry out the 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.

FIA_UAU.1 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 the 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.4 Single-use authentication mechanisms

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

1. Terminal Authentication Protocol

FIA_UAU.4.1/MP_3DES The TSF shall prevent reuse of authentication data related to

1. Authentication Mechanisms based on Triple-DES

FIA_UAU.5 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 Triple-DES

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.5.1/EAC The TSF shall provide

1. Terminal Authentication Protocol in use phase only

2. Secure messaging in MAC-ENC mode

to support user authentication.

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

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

FIA_UAU.5.1/MP_3DES The TSF shall provide

Symmetric Authentication Mechanism based on Triple-DES

(GP in Perso Phase)

to support user authentication.

FIA_UAU.5.2/MP_3DES The TSF shall authenticate any user's claimed identity according to the

The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with the Personalization Agent Key.

FIA_UAU.6 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 Chip Authentication Protocol shall be verified as being sent by the GIS.**

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication protocol according to [R34]** to prove the identity of the **TOE**.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 /EAC The TSF shall enforce the **Access Control SFP** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD.**

FDP_ACF.1 Security attribute based access control

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

1. Subjects:

a. Personalization Agent

b. Extended Inspection System

c. Terminal

2. Objects:

a. Data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD

b. Data EF.DG3 and EF.DG4 of the logical MRTD

c. Data in EF.COM

d. Data in EF.SOD

3. Security attributes

a. Authentication status of terminals

b. Terminal Authorization

FDP_ACF.1.2/EAC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. The successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD

2. The successfully authenticated Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD

3. The successfully authentication Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD

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

FDP_ACF.1.4/EAC The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3**
2. **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4**
3. **A terminal authenticated as DV is not allowed to read data in the EF.DG3**
4. **A terminal authenticated as DV is not allowed to read data in the EF.DG4**
5. **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD**
6. **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD**

FDP_UCT.1 Basic data exchange confidentiality

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

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1/CA 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**.

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

FMT_SMF.1 Specification of Management Functions

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

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

FMT_SMR.1 Security roles

FMT_SMR.1.1/MP The TSF shall maintain the roles

1. **Manufacturer**
2. **Personalization Agent**

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

Application Note: Here the role “Manufacturer” matches the “Prepersonalizer”, i.e. the “MRTD manufacturer”.

FMT_SMR.1.1/TA The TSF shall maintain the roles

1. **Country Verifying Certification Authority**
2. **Document Verifier**
3. **Domestic Extended Inspection System**
4. **Foreign Extended Inspection System**

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

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced**:**

Deploying Test Features after TOE Delivery does not allow

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

FMT_LIM.1.1/EAC 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:

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

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced**:**

Deploying Test Features after TOE Delivery does not allow:

1. **User Data to be manipulated**

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

FMT_LIM.2.1/EAC 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:

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

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1/MP_INI_ENA The TSF shall **restrict** the ability **to write** the **Initialization Data and Prepersonalization Data** to **the Prepersonalizer**.

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

FMT_MTD.1.1/MP_KEY_READ The TSF shall restrict the ability to **read** the **See below** to **See below:**

TSF Data	Authorized Identified roles
MSK	None
Personalization Agent keys	None

FMT_MTD.1.1/TA_CVCA_INI The TSF shall **restrict** the ability **to write** the:

1. **Initial Country Verifying Certification Authority Public Key**
2. **Initial Country Verifying Certification Authority Certificate**
3. **Initial Current Date**

to the **Personalization Agent**

FMT_MTD.1.1/TA_CVCA_UPD The TSF shall **restrict** the ability **to write** the:

1. **Initial Country Verifying Certification Authority Public Key**
2. **Initial Country Verifying Certification Authority Certificate**

to the **Country Verifying Certification Authority**

FMT_MTD.1.1/TA_CVCA_DATE The TSF shall **restrict** the ability **to modify** the **Current date** to:

1. **Country Verifying Certification Authority**

2. **Document Verifier**
3. **Domestic Extended Inspection System**

FMT_MTD.1.1/BAC_KEY_WRITE The TSF shall restrict the ability to **write** the **See below** to **See below:**

TSF Data	Authorized Identified roles
Document Basic Access Keys	**Personalization Agent**

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

FMT_MTD.1.1/BAC_Key_READ The TSF shall **restrict** the ability **to read** the **Document Basic Access Keys** to **none.**

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

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1/EAC [Editorially Refined] The TSF shall ensure that only secure values of **the certificate chain** are accepted for **TSF data of the Terminal Authentication Protocol and the Access Control.**

Refinement:
The Certificate chain is valid if and only if:
1- The digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE
2- The digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE
3- The digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG6 to EF.DG16.**

FPT_EMS.1.2 The TSF shall ensure any **users** are unable to use the following interface **smart card circuit contacts** to gain access to **EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG6 to EF.DG16**.

FPT_EMS.1.1/MP The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Keys** and **MSK and CAK**.

FPT_EMS.1.2/MP The TSF shall ensure any **users** are unable to use the following interface **smart card circuit contacts** to gain access to **Prepersonalizer Key, Personalization Agent Keys and MSK**.

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

FPT_EMS.1.2/CA The TSF shall ensure any **users** are unable to use the following interface **smart card circuit contacts** to gain access to **Chip Authentication: Session Keys, Private Key (CAK).**

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to out-of-range operating conditions where therefore a malfunction could occur
2. Failure detected by TSF according to FPT_TST.1.

FPT_TST.1 TSF testing

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

- **At reset**
- **Before any cryptographic operation**
- **When accessing a DG or any EF**
- **Prior to any use of TSF data**
- **Before execution of any command**

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

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

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:**

- **When performing the Chip Authentication**

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 **TSF executable code**.

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

- **When using the CVCA Root key**
- **When verifying a certificate with an extracted public key µ**
- **When performing a Terminal Authentication**

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

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

FPT_PHP.3 Resistance to physical attack

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

10 TOE SUMMARY SPECIFFICATION

10.1 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 that the access conditions are fulfilled as well as the life cycle state.

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

- BAC keys
- Chip Authentication keys,
- Personalization Agent keys
- MSK
- CVCA certificate

It controls access to the CPLC data as well:

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

Regarding the file structure:

In the operational use:

- The terminal can read user data (except DG3 & DG4), EF.SOD, EF.CVCA, EF.COM only after BAC authentication and through a valid secure channel.
- When the EAC was successfully performed, the terminal can only read the DG3 & DG4 provided the access rights are sufficient and through a valid secure channel.

In the personalization phase

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

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

Access Control in writing

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

This security functionality ensures the application locks can only be written in Prepersonalization and personalization phases.

It ensures as well the writable part of CPLC data cannot be written anymore once the TOE is personalized.

Regarding the file structure

In the operational use:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any system files. However:

- The application data is still accessed internally by the application for its own needs
- The root CVCA key files and temporary key files are updated internally by the application according to the authentication mechanism described in [R16].

In the Prepersonalization and personalization phase:

- 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).

EAC mechanism

This security functionality ensures the EAC is correctly performed.

In particular:

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

It can only be performed once the TOE is personalized with the chip authentication keys & Root CVCA key(s) loaded by the Personalization Agent during the Prepersonalization and personalization phase. Furthermore, this security functionality ensures that the authentication is performed as described in the PP [R10].

The TOE also implements countermeasures to protect the TOE; it takes more and more time for the TOE to reply to subsequent wrong GIS authentication attempts.

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 algorithm. This TSF can use a Secure Messaging described in the TSF Secure Messaging.

Physical protection

This security functionality protects the TOE against physical attacks.

Prepersonalization

This security functionality ensures the TOE, when delivered to the Prepersonalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric

Authentication mechanism based on a Triple DES 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

- an integrity error is detected by F.SELFTESTS
- a tearing occurs (during a copy of data in the memory)

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 and integrity of the channel the TOE and the IFD are using to communicate.

After a successful BAC authentication and successful Chip Authentication, a secure channel is established based on Triple DES algorithm.

This security functionality ensures:

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

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

This TSF also provides a GP Secure Messaging (SCP02) for the Prepersonalization or Personalization.

Self tests

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

- At reset
- Before any cryptographic operation
- When accessing a DG or any EF
- Prior to any use of TSF data
- Before execution of any command
- When performing the Chip Authentication
- When using the CVCA Root key
- When verifying a certificate with an extracted public key

When performing a Terminal Authentication

10.2 Links between SFRs and TSF

This table explicits where PP EAC requirements are implemented.

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4	Implemented in SF
SFR from PP EAC				
FAU_SAS.1		FAU_SAS.1.1/MP		**Prepersonalization**
FCS_CKM.1			FCS_CKM.1.1/CA_DH_SM_DES	**Secure Messaging**
FCS_CKM.4	FCS_CKM.4.1			**Secure Messaging** **EAC mechanism** **Personnalisation**
FCS_COP.1/SHA			FCS_COP.1.1/CA_SHA_SM_3DES FCS_COP.1.1/TA_SHA_RSA	**Prepersonalization** **Personnalisation** **EAC mechanism**
FCS_COP.1/SYM			FCS_COP.1.1/CA_SYM_SM_3DES	**Secure Messaging**
FCS_COP.1/MAC			FCS_COP.1.1/CA_MAC_SM_3DES	**Prepersonalization** **EAC mechanism** **Secure Messaging**
FCS_COP.1/SIG_VER			FCS_COP.1.1/TA_SIG_VER_RSA	**Secure Messaging** **EAC mechanism**
FCS_RND.1	FCS_RND.1.1			**Prepersonalization** **EAC mechanism** **Personalization** **Secure Messaging** **Self tests**

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4	Implemented in SF
FIA_UID.1			FIA_UID.1.1/CA FIA_UID.1.2/CA	**Prepersonalization** **Access Control in reading** **EAC mechanism** **Secure Messaging**
FIA_UAU.1			FIA_UAU.1.1/CA FIA_UAU.1.2/CA	**Access Control in reading** **EAC mechanism** **Secure Messaging**
FIA_UAU.4		FIA_UAU.4.1/MP_3DES	FIA_UAU.4.1/TA	**Access Control in reading** **EAC mechanism** **Secure Messaging**
FIA_UAU.5			FIA_UAU.5.1/CA_3DES FIA_UAU.5.2/CA_3DES FIA_UAU.5.1/EAC FIA_UAU.5.2/EAC FIA_UAU.5.1/MP_3DES FIA_UAU.5.2/MP_3DES	**Access Control in reading** **EAC mechanism** **Secure Messaging**
FIA_UAU.6			FIA_UAU.6.1/CA	**Access Control in reading** **EAC mechanism** **Secure Messaging**
FIA_API.1			FIA_API.1.1/CA	**EAC mechanism**
FDP_ACC.1			FDP_ACC.1.1/EAC	**Access Control in reading** **Access Control in writing**
FDP_ACF.1			FDP_ACF.1.1/EAC FDP_ACF.1.2/EAC FDP_ACF.1.3/EAC FDP_ACF.1.4/EAC	**Access Control in reading** **EAC mechanism**
FDP_UCT.1			FDP_UCT.1.1/CA	**Access Control in reading** **EAC mechanism**
FDP_UIT.1			FDP_UIT.1.1/CA FDP_UIT.1.2/CA	**Access Control in reading** **EAC mechanism**

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4	Implemented in SF
FMT_SMF.1		FMT_SMF.1.1/MP		**Prepersonalization** **Personalization** **Access Control in writing** **Safe state management**
FMT_SMR.1		FMT_SMR.1.1/MP FMT_SMR.1.2/MP	FMT_SMR.1.1/TA FMT_SMR.1.2/TA	**Safe state management**
FMT_LIM.1	FMT_LIM.1.1		FMT_LIM.1.1/EAC	**Safe state management** **Physical protection**
FMT_LIM.2	FMT_LIM.2.1		FMT_LIM.2.1/EAC	**Safe state management** **Physical protection**
FMT_MTD.1/INI_ENA		FMT_MTD.1.1/MP_INI_ENA		**Prepersonalization** **Access Control in writing** **Personalization**
FMT_MTD.1/INI_DIS		FMT_MTD.1.1/MP_INI_DIS		**Access Control in reading**
FMT_MTD.1/CVCA_INI			FMT_MTD.1.1/TA_CVCA_INI	**Access Control in writing**
FMT_MTD.1/CVCA_UPD			FMT_MTD.1.1/TA_CVCA_UPD	**Access Control in writing** **EAC mechanism**
FMT_MTD.1/CVCA_DATE			FMT_MTD.1.1/TA_CVCA_DATE	**Access Control in writing** **EAC mechanism**
FMT_MTD.1/KEY_WRITE			FMT_MTD.1.1/BAC_KEY_WRITE	**Access Control in writing**
FMT_MTD.1/CAPK			FMT_MTD.1.1/CAPK	**Access Control in writing**
FMT_MTD.1/KEY_READ		FMT_MTD.1.1/MP_KEY_READ	FMT_MTD.1.1/BAC_KEY_READ FMT_MTD.1.1/CA_KEY_READ	**Access Control in reading**
FMT_MTD.3			FMT_MTD.3.1/EAC	**Access Control in reading** **EAC mechanism**
FPT_EMS.1	FPT_EMS.1.1 FPT_EMS.1.2	FPT_EMS.1.1/MP FPT_EMS.1.2/MP	FPT_EMS.1.1/CA FPT_EMS.1.2/CA	**Prepersonalization** **EAC mechanism** **Personnalisation**

SFR family	Generic Phases 2,3 & 4	Phases 2 & 3	Phase 4	Implemented in SF
FPT_FLS.1	FPT_FLS.1.1			**Safe state management**
FPT_TST.1	FPT_TST.1.1 FPT_TST.1.2 FPT_TST.1.3		FPT_TST.1.1/CA FPT_TST.1.2/CA FPT_TST.1.3/CA FPT_TST.1.1/TA FPT_TST.1.2/TA FPT_TST.1.3/TA	**Self tests**
FPT_PHP.3	FPT_PHP.3			**Physical protection**

Table 12 - Links between SFR and TSF

Application NOTE: the ADV_FSP and ATE documents explicit more precisely how to get the links between SFR and Oberthur Technologies specifications.

11 RATIONALES

The rationales are available in the complete ST.

Appendix A: Glossary

Acronym	Definition
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 fonction