ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE

Public Security Target

FQR No: 110 7965

FQR Issue: 4

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Document Management

A. Identification

Business Unit - Department	CAI R&D
Document type:	FQR
Document Title:	ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE – Public Security Target
FQR No:	110 7965
FQR Issue:	4

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

Table of contents

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

List of Figures

List of tables

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1 SECURITY TARGET INTRODUCTION

1.1 Purpose

The objective of this document is to present the Public Security Target of ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE.

1.2 Objective of the security target

This security target describes the security needs for ID-One ePass Full EAC v2 MRTDproduct. The product is conforming to PP PACE and adds requirements for prepersonalization and personalization.

This security target aims to satisfy the requirements of Common Criteria level EAL5 augmented as defined in §1.3 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.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1.3 Security target identification

Title:	**MINOS – ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE – Security Target**
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL5 augmented with: - ALC_DVS.2 - AVA_VAN.5
PP(s):	BSI-CC-PP-0068 v2 [R14]
ST Reference:	FQR 110 7888 Issue 4
ITSEF:	LETI
Certification Body:	ANSSI
Evaluation scheme:	FR

Table 1 - General Identification

1.4 TOE technical identification

Product name:	**ID-One ePass Full EAC v2**
Commercial name of the TOE:	**ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on P60x144 PVA/PVE**
IC type	‘6A15’ (P60D144 VA) ‘6A20’ (P60C144 VA) ‘6E15’ (P60D144 VE) ‘6E20’ (P60C144 VE)
Additional code 1 Mandatory generic Identification:	‘082458FFF905CCCB2DB3F14012A0245840BEA310081875D3851D6F4DD1923AE450D8A55D’
Additional code 2 Optional DBI Identification:	‘082845FF62EF601FB487C51B4D653D85C94DE1BC30A13B71C5C0F457516CDAB27FFB696C’
Guidance document	MINOS - ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM - Guidance Document - PREparative procedures FQR 110 7929 Issue 4 MINOS - MRTD full EAC v2 - Guidance Document - OPErational user guidance FQR 110 7565 Issue 3

Table 2 - TOE Technical Identification

Nota Bene

- The additional code is encrypted with the LSK key
- An optional additional code (functional) can be loaded. This additional code, relative to the Digitally Blurred Image process (DBI) is part of the product, but not in the scope of the evaluation.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1.5 IC identification

IC Reference:	NXP P60 chips
TOE:	NXP P60x144/080 PVA/PVE (Y) [R18] EAL 6 augmented by ASE_TSS.2, ALC_FLR.1
Communication protocol:	Contact, Contactless and Dual
Memory:	ROM
Chip Manufacturer:	NXP Semiconductors

Table 3 - Chip Identification

2 TOE OVERVIEW

2.1 Product overview

The product **ID-One Native eDoc** is a 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]**. It also provides standard authentication protocols, namely Basic Access Control **[R11]**, Supplementary Access Control **[R17]**, Active Authentication [R38], Extended Access Control (**[R12]** and **[R13]**), the Basic Access Protection **[R9]** and Extended Access Protection (compliant to **[R9]**).

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

This product is embedded on the ICs described in §1.5 IC identification.
The **ID-One Native eDoc** architecture can be viewed as shown in the following picture:

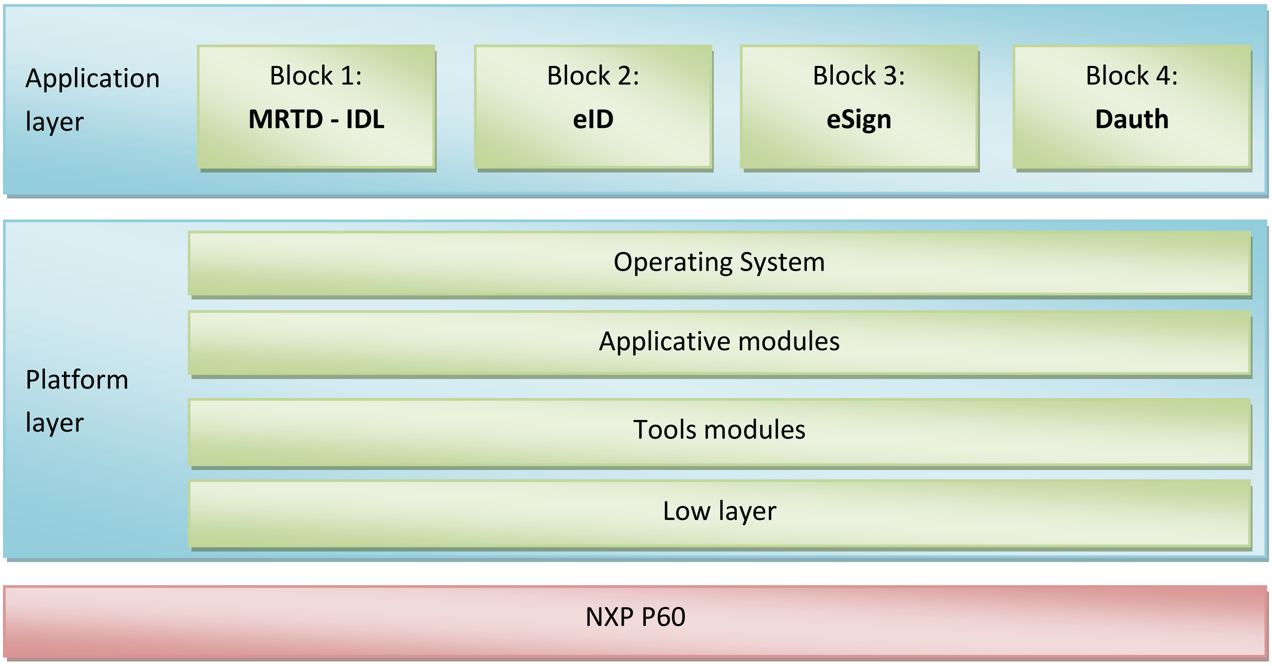

Figure 1 - ID-One Native eDoc Overview

2.2 TOE overview

The TOE described in this security target is the PACE with CA, PACE_CAM and AA TOE of the product, a subset of the Block 1 MRTD - IDL.

The block 1 of the ID-One Native eDoc is composed of the following applications:

Applications	PP	Targeted EAL
MRTD		
BAC with CA and AA	**[R11]**	EAL4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_DVS.2 + ALC_CMS.5 + ALC_TAT.2 + ATE_DPT.3
EAC with AA	**[R12]**	EAL5 + ALC_DVS.2 + AVA_VAN.5
EAC with PACE and AA	**[R13]**	EAL5 + ALC_DVS.2 + AVA_VAN.5
PACE with CA, PACE_CAM and AA	**[R14]**	EAL5 + ALC_DVS.2 + AVA_VAN.5
IDL		
BAP	X	EAL4 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_DVS.2 + ALC_CMS.5 + ALC_TAT.2 + ATE_DPT.3
EAC and BAP	X	EAL5 + ALC_DVS.2 + AVA_VAN.5
PACE	X	EAL5 + ALC_DVS.2 + AVA_VAN.5

Applications	PP	Targeted EAL
PACE and EAC	X	EAL5 + ALC_DVS.2 + AVA_VAN.5

Table 4 - Block 1 Applications overview

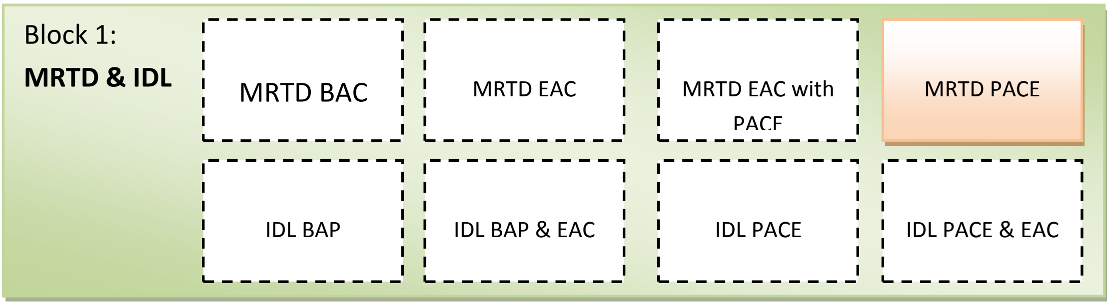

Figure 2 - Block 1 Overview

The PACE with CA, PACE_CAM and AA TOE is instantiated during the product prepersonalization, using the operating system that creates the MF / DF required for the PACE configuration.

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

The TOE identification is described in **§1.4** TOE technical identification**.**

Nota bene

The TOE scope encompasses the following features:

- PACE (Password Authenticated Connection Establishment)
- Chip Authentication
- PACE CAM (Password Authenticated Connection Establishment with Chip Authentication Mapping)
- Active Authentication
- Prepersonalization phase
- Additional code loading

Nevertheless, the TOE can embed other secure functionalities, but they are not in the scope of this TOE and subject to an evaluation in other TOEs.

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
- A separate data summary (MRZ or keydoc data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ or keydoc area)
- And data elements stored on the TOE's chip for contact-less machine reading.

The authentication of the holder is based on:

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

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

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

The MRTD can be viewed as the combination:

- **A physical MRTD** in form of paper or plastic with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to) personal data of the MRTD holder
    - The biographical data on the biographical data page of the passport book
    - The printed data in the Machine-Readable Zone (MRZ) or keydoc area that identifies the device
    - The printed portrait
- **A logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure as specified by ICAO and extended in **[R7]**, **[R8]**, **[R9]** on the contactless integrated circuit. It presents contact or contact-less readable data including (but not limited to) personal data of the MRTD holder
    - The digital Machine Readable Zone Data (digital MRZ data or keydoc data, DG1)
    - The digitized portraits
    - The optional biometric reference data of finger(s) or iris image(s) or both
    - The other data according to LDS (up to DG24)

- The Document security object

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The MRTD as the physical device and the MRTD's chip is uniquely identified by the document number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organisational security measures (e.g. control of materials, personalization procedures). These security measures include the binding of the MRTD's chip to the physical support.

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

2.4 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providingthe following features:

- Active Authentication
- Chip Authentication
- PACE
- PACE CAM

The TOE comprises at least:

- Circuitry of the MRTD's chip (the integrated circuit, IC)
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- IC Embedded Software (operating system)
- MRTD application
- Associated guidance documentation

3 TOE ARCHITECTURE

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

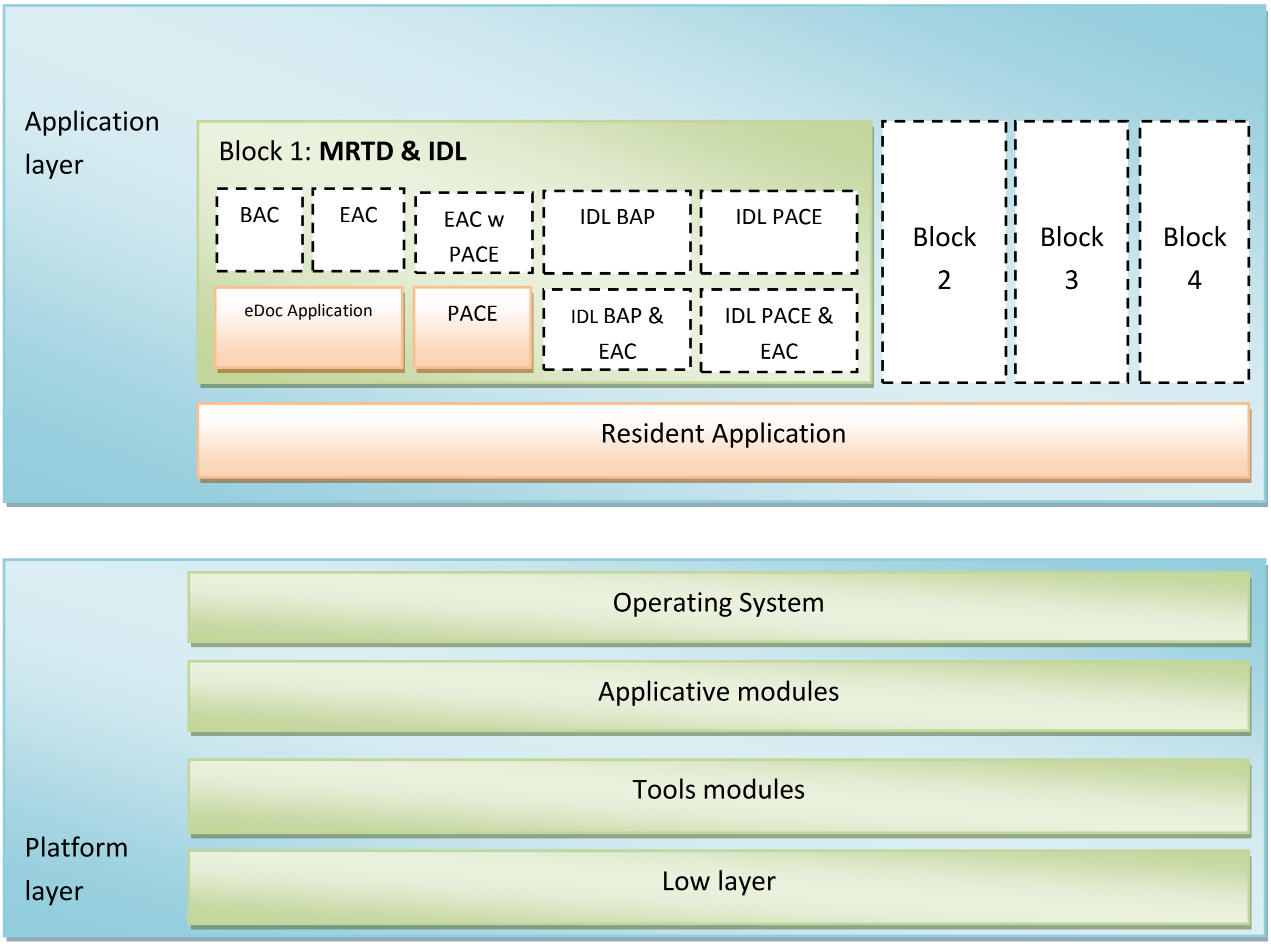

Figure 3 - TOE architecture

3.1 Integrated Circuit - NXP P60

The TOE is embedded on NXP chips, as presented in **Table 3 - Chip Identification.**
More information on the chips are given in the related security targets.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.2 Low layer

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

The main features of the OS are the following:

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

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, SHA-384 and SHA-512 bits	✓
RSA CRT from 1024, to 4096 bits (by steps of 256 bits): - signature/verification - key pair generation	✓
RSA SFM from 1024 to 4096 bits (by steps of 256 bits): - signature/verification - key pair generation	✓
ECC with key sizes from 192 to 521 bits : - signature/verification (ECDSA) - key agreement (ECDH) - key pair generation	✓
3DES with 112 bits key size	✓
AES with 128, 192, 256 key sizes	✓
Random Generator compliant AIS31	✓
Diffie Hellman from 1024 to 2048 : - key agreement - key generation	✓
Integrated mapping over prime field and Elliptic curves	✓

Table 5 - OT Cryptographic library

More information is available in complete ST.

3.3 Tools modules

The tools modules provide MRTD full EAC v2 product:

- File system compliant with ISO/IEC 7816-4 and ISO/IEC 7816-9. It is also compliant with ICAO recommendations **[R2]**.
- ISO Secure Messaging as specified in **[R19]** and as described in annex E of **[R40]**.
- PIN and BIO access rights management as presented in § 2.5 of **[R39]** and B.6 of **[R40]**
- 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.

3.4 Applicative modules

The applicative modules provide MRTD full EAC v2 product:

- Chip Authentication version 1 as described in **[R38]** and version 2 as described in **[R39]**, an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.
- Terminal Authentication version 1 as described in **[R38]** and version 2 as described in **[R39]**, a two move challenge-response protocol that provides explicit unilateral authentication of the terminal.
- PACE Protocol as specified in **[R17]**, a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and explicit password-based authentication of the MRTD chip and the terminal.
- Access Conditions Engine that checks the AC rules attached to an object (file, key, data object) with a current context (CHA, Role ID…). For applications already defined by normative documents such as eMRTD, iDL, eID and eSign, the application embeds ROMed access condition rules.
- 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. This module is part of the TOE and outside the scope of this present certification.

More information is available in complete ST.

3.5 Operating System

This application 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, LSK), File management including data reading and writing or additional code loading. It can be addressed in clear mode for secure environment or non-sensitive commands, using SCP02 or SCP03.

More information is available in complete ST.

3.6 Application layer

Two kinds of dispatcher are available on the top of the product: the resident application that is used for Personalization Phase and for administration during Use Phase and the eDoc application that is used during the Use Phase of MRTD Applications.

The application layer also manages protocols available during Use phase such as Basic Access Control Extended Access Control, Password Authenticated Connection Establishment 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 **[R35]** 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.

The protocol for Basic Access Control is specified by ICAO. 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 **[R35]** 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.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The Extended Access Control (EAC) enhances the latest security features and ensures a strong and mutual authentication of the TOE and the Inspection system. This step is required to access biometric data such as fingerprints and iris stored in DG3 and DG4. In particular, the authentication steps ensures a strong secure channel able to provide confidentiality of the biometric data that are read and authentication of the Inspection system retrieving the date to perform a Match on Terminal comparison. The Extended Access Control authentication steps may be performed either with elliptic curve cryptography, or with RSA cryptography.
This application uses the Chip Authentication and then after the Terminal Authentication.

The Password Authenticated Connection Establishment (PACE) is a security feature that is supported by the TOE.
The Inspection System:

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

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

More information is available in complete ST.

4 TOE LIFE CYCLE

4.1 Life cycle overview

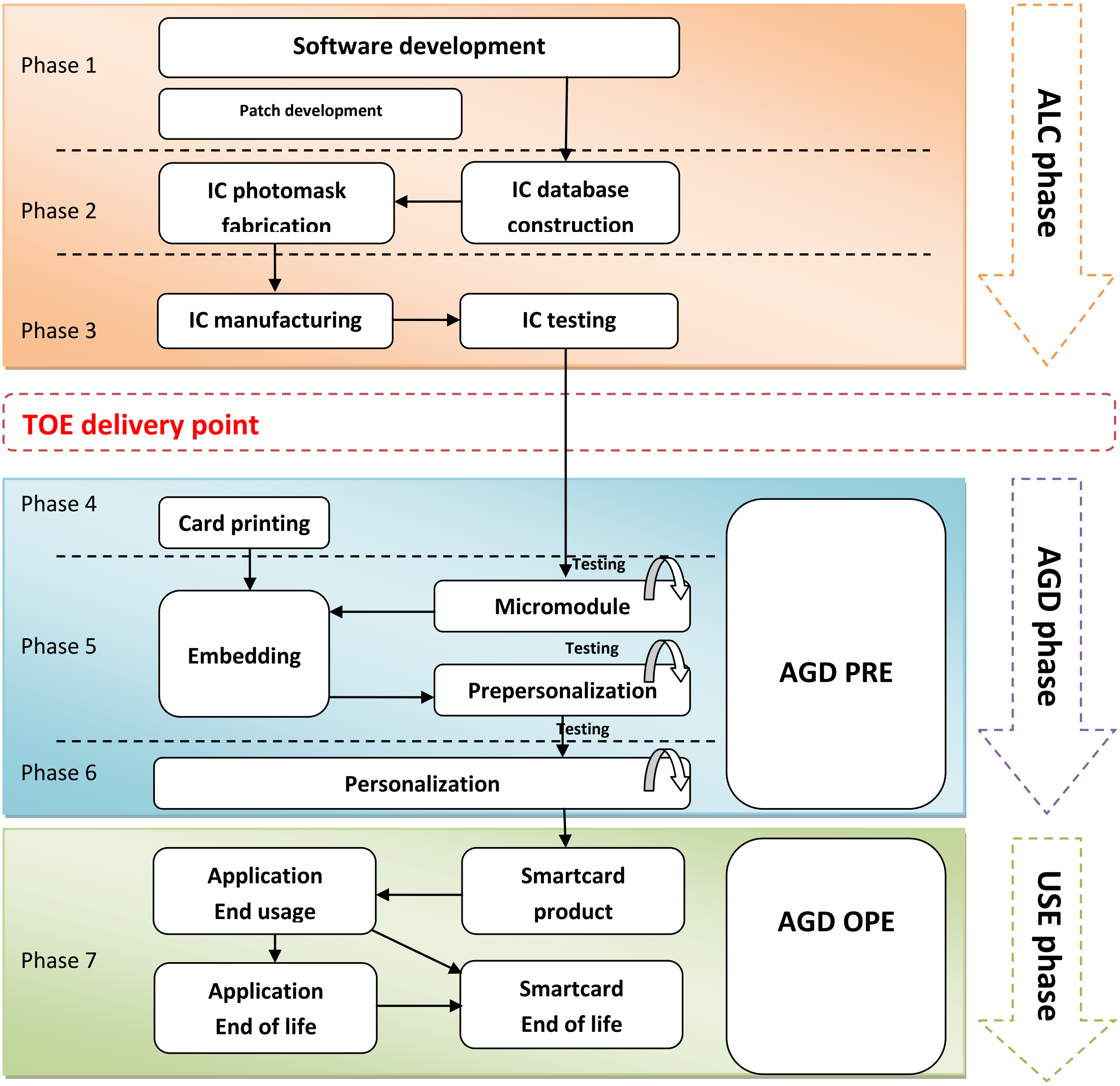

Figure 4: Smartcard product life-cycle for the TOE

The TOE life-cycle is described in terms of four life-cycle phases. (With respect to the **[R10]**, the TOE life-cycle is additionally subdivided into 7 steps.)

Additional codes are identified in §1.5**.**

The table below presents the TOE role:

Roles	Subject
IC developer	NXP Semiconductors
IC manufacturer	NXP Semiconductors
TOE developer	Oberthur Technologies
Manufacturer	NXP Semiconductors Oberthur Technologies or another agent
Prepersonalizer	Oberthur Technologies or another agent
Personalization Agent	Oberthur Technologies or another agent

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 **[R10]**, the Protection Profile lifecycle in phases, the TOE delivery point and the coverage:

Steps	Phase	Subject	Covered by	Sites
Step 1	Development	Oberthur Technologies	ALC R&D sites	Pessac and Colombes
Step 2	Development	NXP Semiconductors	IC certification	IC certification
Step 3	Manufacturing	NXP Semiconductors	IC certification	IC certification
TOE delivery point				
Step 4	Manufacturing	MRD Manufacturer (Prepersonalizer)	AGD_PRE	
Step 5	Manufacturing	MRD Manufacturer (Prepersonalizer)	AGD_PRE	
Step 6	Personalization	Personalization Agent	AGD_PRE	
Step 7	Operational Use	End user	AGD_OPE	

Table 7 - Subjects identification following life cycle steps

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

4.3 Phase 2 "Manufacturing"

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

TOE delivery point

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

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

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

Additional code loading is performed in Prepersonalization phase. It is compliant to ANSSI Note 6 **[R44]**.

The additional code loading process is performed by the Prepersonalizer in the following steps, via the Command LOAD SECURE:

- Additional code generation
- MSK authentication
- LSK derivation
- Memory area definition
- Loading of the additional code
- Secure activation of the additional code

The additional code loading is performed before the creation of the MF file during Prepersonalization.

Identification of the additional code loading is given in Table 2 - TOE Technical Identification.

Additional code generation

The additional code is generated by Oberthur Technologies: developped, compiled, ciphered and signed. After generation, it is sent to the MRTD manufacturer to that it can load it in the (initial) TOE.

Loading of the additional code

The additional code is loaded in the (initial) TOE by the Prepersonalizer that shall authenticate itself to the TOE beforehand. Upon reception, the (intial) TOE checks it has been generated by Oberthur Technologies (by verifying the signature) before activating it.

Identification of the TOE

After successful loading and activation of the additional code, the TOE update its identification data to reflects the presence of the additional code.

4.4 Phase 3 "Personalization of the travel document"

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

4.5 Phase 4 “Operational Use”

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

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

5 CONFORMANCE CLAIMS

5.1 Common Criteria conformance

This Security Target (ST) claims conformance to the Common Criteria version 3.1 revision 4 **[R41]**, **[R42]** and **[R43]**.

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 5, augmented with: - ALC_DVS.2 *"Sufficiency of security measures"* - AVA_VAN.5 *"Advanced methodical vulnerability analysis"*

Table 8 - Conformance Rationale

5.1.1 Overview of the SFR defined in this ST

SFR are presented in **§ 9.1 Security Functional Requirements**:

- SFR (/Global) that are global to the product (shared between the various TOE)
- SFR (/MP_Add_code) that are dedicated for the patch loading
- SFR (/MP) that are dedicated for the Manufacturing and Personalization phases
- SFR (/AA) that are dedicated for Active Authentication
- SFR (/PACE) that are dedicated for Password Authenticated Connection Establishment
- SFR (/PACE_CAM) that are dedicated for Password Authenticated Connection Establishment with Chip Authentication Mapping

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

[1] *The rationale for SFR addition is described in the relative PP and in this Security Target*

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

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

Table 9 -SFR from the PP

Section	Additional SFR
MP	FCS_CKM.1/MP ; FCS_COP.1/MP ; FDP_ACC.2/MP ; FDP_ACF.1/MP ; FDP_ITC.1/MP ; FDP_UCT.1/MP ; FDP_UIT.1/MP ; FIA_AFL.1/MP ; FIA_UAU.1/MP ; FIA_UID.1/MP ; FIA_UAU.4/MP ; FIA_UAU.5/MP ; FMT_MTD.1/MP ; FTP_ITC.1/MP ; FMT_MTD.1/MP_KEY_READ ; FMT_MTD.1/MP_KEY_WRITE
MP Add code	FAU_STG.2/MP_Add_code ; FTP_ITC.1/MP_Add_code ; FCS_CKM.1/MP_Add_code ; FCS_COP.1/MP_Add_code ; FDP_UIT.1/MP_Add_code ; FMT_MTD.1/MP_Add_code ; FMT_MTD.1/MP_KEY_READ_Add_code ; FMT_SMR.1/MP_Add_code
Active Authentication	FCS_COP.1/AA ; FDP_DAU.1/AA ; FDP_ITC.1/AA ; FMT_MTD.1/AA_KEY_READ ; FMT_MOF.1/AA ; FMT_MTD.1/AA_KEY_WRITE
PACE CAM	FIA_UAU.1/PACE_CAM; FIA_UAU.4/PACE_CAM; FIA_UAU.5/PACE_CAM; FIA_UAU.6/PACE_CAM; FIA_UID.1/PACE_CAM; FMT_MTD.1/CA_KEY_WRITE

Table 10 - Additional SFR

5.1.2 Overview of the additional protocols

5.1.2.1 Active Authentication

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

- Additional Threats: **§ 6.3.3 Threats for AA**
- Additional Objective: **§ 7.1.3 SO for AA**
- Additional OE: **§ 7.2.3 OE for AA**

5.1.2.2 Prepersonalization phase

The prepersonalization phase has been reinforced in this Security Target, with the following elements.

This functionality is usable in phase 5 and phase 6. Once the product is locked, stated as personalized, it is no more possible to perform this operation. The following addition has been performed:

- Additional Threats: **§ 6.3.4 Threats for Note 6**
- Additional Objective: **§ 7.1.4 SO for Note 6**

The TOE is compliant to the last version (draft) of ANSSI Note 6 **[R44]**.

5.1.2.3 PACE CAM

The additional functionality of Password Authenticated Connection Establishment with Chip Authentication Mapping (PACE CAM) has been added to the TOE.
It possesses the same security requirements than the PACE functionality, that means that the same SPD applies to the PACE CAM.
Additional SFR has been defined for defining the PACE CAM security functional requirements.

5.2 Protection Profile conformance

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

BSI-CC-PP-0068-V2-2011:"Machine Readable Travel Document using Standard Inspection Procedure with PACE" [R14].

5.3 Rationale for the additions

The rationales are available in the complete ST.

5.4 Non evaluated features

In order to be powered up and to communicate with the 'external world' the TOE needs a terminal (card reader) supporting the contactless/contact based communication according to [7]and [8]. From the logical point of view, the TOE shall be able to recognise the following terminal type, which, hence, shall be available:

- Basic Inspection System with PACE

The TOE shall require terminals to evince possessing authorisation information (a shared secret) before access according to [4], option 'PACE' is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

In scope of this Protection Profile the following types of inspection systems shall be distinguished:

- BIS-PACE: Basic Inspection System with PACE
- BIS-BAC: Basic Inspection System with BAC

The current PP defines security policy for the usage of onlyBasic Inspection System with PACE (BIS-PACE) in the context of the ePassport application.

Using other types of inspection systems and terminals is out of the scope of the current PP. Some developers might decide to implement their products being downwardly compatible with ICAO-terminals, so that they also functionally support Basic Access Control (BAC). However, any product using BAC will not be conformant to the current PP; i.e. a product implementing the TOE may functionally use BAC, but, while performing BAC, they are acting outside of security policy defined by the current PP. Therefore, organisations being responsible for the operation of inspection systems shall be aware of this context.

Some features may be part of the TOE but are not evaluated as they are not relevant for the TSFs:

- Standard and biometric PIN management
- File system management
- DBI

The TOE may also contain other applications such as eID, eSign, …..The current evaluation covers any combination of application.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6 SECURITY PROBLEM DEFINITION

6.1 Subjects

6.1.1 PP PACE subjects

Travel document holder (MRTD holder)
A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [R11]. Please note that a travel document holder can also be an attacker.

Travel document presenter (Traveler)
A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [R11]. Please note that a travel document presenter can also be an attacker (s. below).

Terminal
A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [R11].

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

Document Signer (DS)
An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA
issuing the Document Signer Certificate (CDS), see [R2]. This role is usually delegated to a Personalisation Agent.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Country Signing Certification Authority (CSCA)

An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI.

The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [R2].

Personalisation Agent

An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:

(i) Establishing the identity of the travel document holder for the biographic data in the travel document

(ii) Enrolling the biometric reference data of the travel document holder

(iii) Writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [R2]

(iv) Writing the document details data

(v) Writing the initial TSF data

(vi) Signing the Document Security Object defined in [R2] (in the role of DS).

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

This entity is commensurate with 'Personalisation agent' in [R11].

Application Note

Personalization Agent is refered as the Personalizer in the Security Target

Manufacturer

Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.

This entity is commensurate with 'Manufacturer' in [R11].

Attacker

A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential.

Please note that the attacker might 'capture' any subject role recognised by the TOE.
This external entity is commensurate with 'Attacker' in [R11].

6.1.2 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 [R11].

6.2 Assets

6.2.1 Primary assets

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

User data stored on the TOE
Protection: Confidentiality, Integrity, Authenticity
All data (being not authentication data) stored in the context of the eMRTD application of the travel document as defined in **[R2]** and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of **[R2]**)
This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in **[R11].**

User Data	Description
CPLC Data	Data uniquely identifying the chip. They are considered as user

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

Table 1: User data stored on the TOE

User data transferred between the TOE and the terminal connected
Protection: Confidentiality, Integrity, Authenticity
All data (being not authentication data) being transferred in the context of the eMRTD application of the travel document between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of **[R2]**).
User data can be received and sent (exchange <--> [receive, send]).

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

6.2.2 Secondary assets

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

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

	confidentiality and in integrity

Table 2: Accessibility to the TOE functions and data only for authorised subjects

Genuineness of the TOE

Protection: Availability

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD chip'' in **[R11].**

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

Table 3: Genuineness of the TOE

TOE internal secret cryptographic keys

Protection: Confidentiality, Integrity

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

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

TSF data	Description
LSK	Loading Secure Key used to load Optional Code in pre-personalisation phase

Table 4: TOE internal secret cryptographic keys

TOE internal non-secret cryptographic material

Protection: Confidentiatity, Integrity

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

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

Table 5: TOE internal non-secret cryptographic material

Travel Document communication establishment authorisation data

Protection: Confidentiatity, Integrity

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

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

Table 6: Travel Document communication establishment authorisation data

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.

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

6.3.1 Threats from the PP PACE

T.Skimming

Adverse action

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

Threat agent

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

Asset

Confidentiality of logical travel document data

T.Eavesdropping

Adverse action

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

Threat agent

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

Asset

Confidentiality of logical travel document data

T.Tracing

Adverse action

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

Threat agent

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

Asset

Privacy of the travel document holder

T.Forgery

Adverse action

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

Threat agent

Having high attack potential

Asset

Integrity of the travel document.

T.Abuse-Func

Adverse action

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

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

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

Threat agent

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

Asset

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

T.Information_Leakage

Adverse action

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

Threat agent

Having high attack potential

Asset

Confidentiality of User Data and TSF data of the travel document

T.Phys-Tamper

Adverse action

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

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

An attacker may physically modify the MRTD's chip in order to alter

(i) Its security functionality (hardware and software part, as well)
(ii) The user Data or the TSF data stored on the MRTD

Threat agent

Having high attack potential, being in possession of a legitimate MRTD.

Asset

Integrity and authenticity of logical MRTD, availability of the functionality of the MRTD, confidentiality of User Data and TSF-data of the MRTD

T.Malfunction

Adverse action

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

(i) Deactivate or modify security features or functions of the TOE
(ii) Circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent

Having high attack potential, being in possession of one or more legitimate MRTD, having information about the functional operation

Asset

Integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

6.3.2 Threats for CA

T.Counterfeit

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

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

Asset: authenticity of logical MRTD data

6.3.3 Threats for AA

T.Counterfeit

6.3.4 Threats for Note 6

T.Unauthorized_Load

Adverse action

An attacker tries to load an additional code that is not intended to be assembled with the initial TOE, ie the evidence of authenticity or integrity is not correct.

Threat agent

Having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate MRTD

Asset

Logical MRTD data

T.Bad_Activation

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Adverse action

An attacker tries to perturbate the additional code activation such as the final TOE is different than the expected one (initial TOE or perturbated TOE).

Threat agent

Having high attack potential, knowing the MSK, LSK and derivation data, being in possession of a legitimate MRTD, being in possession of an additional code that is authorized to be load

Asset

Logical MRTD data

T.TOE_Identification_Forgery

Adverse action

An attacker tries to perturbate the TOE identification and in particular the additional code identification.

Threat agent

Having high attack potential, being in possession of a legitimate MRTD

Asset

TOE_ID

Application Note: This threat is not applicable in phase 7, as the TOE identification is not possible in phase 7.

6.4 Organisational Security Policies

6.4.1 OSP from PP PACE

P.Manufact

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

P.Pre-Operational

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

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

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

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

P.Card_PKI

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

2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [R17]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issue.

3) A Document Signer shall:

(i) Generate the Document Signer Key Pair
(ii) Hand over the Document Signer Public Key to the CSCA for certification
(iii) Keep the Document Signer Private Key secret
(iv) Securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworthy_PKI

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

P.Terminal

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

1) The related terminals shall be used by terminal operators and by travel document holders

2) They shall implement the terminal parts of the PACE protocol [R17], of the Passive Authentication [R2] and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann)

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

4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [R2])

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

6.4.2 OSP for CA

P.Chip_Auth
The terminal implements the Chip Authentication protocol as described in [R38].

6.4.3 OSP for AA

P.Activ_Auth
The terminal implements the Active Authentication protocol as described in **[R38]**.

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.

The Assumptions are taken from the PP EAC with PACE, which requires to include also some Assumptions described in the PP PACE.

6.5.1 Assumptions from PP PACE

A.Passive_Auth

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

The Document Signer

(i) Generates the Document Signer Key Pair
(ii) Hands over the Document Signer Public Key to the CA for certification
(iii) Keeps the Document Signer Private Key secret
(iv) Uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [R10].

6.5.2 Assumptions for Chip Authentication

A.Insp_Sys_CA

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

A.Signature_PKI

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations.

6.5.3 Assumptions for Active Authentication

A.Insp_Sys_AA

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

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.

7.1.1 SO from PP PACE

OT.Data_Int

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

OT.Data_Auth

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

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

OT.Data_Conf

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected.

The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Application note:

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

OT.Prot_Abuse-Func

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

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

OT.Prot_Inf_Leak

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

- 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
- Forcing a malfunction of the TOE and/or
- A physical manipulation of the TOE.

Application note:

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

OT.Prot_Phys-Tamper

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software by means of:

- Measuring through galvanic contacts representing a direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- Measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis)
- Manipulation of the hardware and its security 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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

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

OT.Identification

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

OT.AC_Pers

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [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.

Application note:

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

7.1.2 SO for CA

OT.CA_Proof

The TOE must support the Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [R38]. The authenticity proof provided by the MRTD's chip shall be protected against attacks with high attack potential.

Application note

The objective implies the MRTD's to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [R2] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.Data_Int_CA

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

7.1.3 SO for AA

OT.AA_Proof

The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [R2]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

OT.Data_Int_AA

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

7.1.4 SO for Note 6

OT.Secure_Load_ACode

The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE.

During the Load Phase of an Additional Code, the TOE shall remain secure.

OT.Secure_AC_Activation

Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation.

If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.

OT.TOE_Identification
The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user must be able to uniquely identify Initial TOE and Addtitional Code(s) which are embedded in the Final TOE. TOE must support the Inspection Systems to verify the authenticity.

7.2 Security objectives for the Operational Environment

7.2.1 OE from PP PACE

7.2.1.1 Travel document Issuer ad the general responsible

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

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

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

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

(i) generate a cryptographically secure Document Signing Key Pair

(ii) ensure the secrecy of the Document Signer Private Key

(iii) hand over the Document Signer Public Key to the CSCA for certification

(iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [6].

The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [6]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct DocumentSecurity Objects to be stored on travel document.

OE.Personalization

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf:

(i) establish the correct identity of the travel document holder and create the biographical data for the travel document

(ii) enrol the biometric reference data of the travel document holder

(iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [R2]

(iv) write the document details data

(v) write the initial TSF data

(vi) sign the Document Security Object defined in [R2] (in the role of a DS).

OE.Terminal

The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [R2]

2.) The related terminals implement the terminal parts of the PACE protocol [R3], of the Passive Authentication [R3] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann)

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

4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCAand CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [R2])

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

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

7.2.2 OE for CA

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

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

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

Application note
The Inspection Systems 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 PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication.

7.2.3 OE for AA

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

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

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

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

(i) Generate the MRTD's Active Authentication Key Pair
(ii) Ensure the secrecy of the MRTD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15
(iii) Support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object

8 EXTENDED REQUIREMENTS

8.1 Extended family FAU_SAS - Audit data storage

8.1.1 Extended components FAU_SAS.1

Description: see **[R11]**.

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 **[R11]**

8.2 Extended family FCS_RND - Generation of random numbers

8.2.1 Extended component FCS_RND.1

Description: see **[R11]**

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 **[R11]**

8.3 Extended family FIA_API – Authentication proof of identity

8.3.1 Extended component FIA_API.1

Description: see **[R12]**

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

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 **[R12]**

8.4 Extended family FMT_LIM - Limited capabilities and availability

8.4.1 Extended component FMT_LIM.1

Description: see **[R11]**

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 **[R11]**

8.4.2 Extended component FMT_LIM.2

Description: See **[R11]**

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)

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Rationale: See **[R11]**

8.5 Extended family FPT_EMS - TOE Emanation

8.5.1 Extended component FPT_EMS.1

Description: see **[R11]**

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 **[R11]**

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com

9 SECURITY REQUIREMENTS

9.1 Security Functional Requirements

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

- **Global SFR** that are applicable to all the passports configuration
- **MP SFR** for covering the phase Manufacturing and Personalization described in the Passport Protection Profile and also the coverage of Additional Code.
- **Active Authentication SFR** that cover the Active Authentication Protocol
- **CA SFR** that cover the Chip Authentication Protocol
- **PACE SFR** that cover the Password Authenticated Connection Establishment protocol
- **PACE CAM** that cover the Password Authenticated Connection Establishment with Chip Authentication Mapping protocol

9.1.1 Global SFR

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

FCS_CKM.4/Global Cryptographic key destruction

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

FCS_RND.1/Global Quality metric for random numbers

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

1. The requirement to provide an entropy of at least 7.976 bits in each byte, following AIS 31 [R36] and

2. The requirement of RGS_B1 for random number generation.

FMT_LIM.1/Global Limited capabilities

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

Deploying Test Features after TOE Delivery does not allow

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com

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

FMT_LIM.2/Global Limited availability

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

Deploying Test Features after TOE Delivery does not allow
1. User Data to be manipulated
2. TSF data to be disclosed or manipulated
3. Software to be reconstructed
4. Substantial information about construction of TSF to be gathered which may enable other attacks

FPT_EMS.1/Global TOE Emanation

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

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

FPT_FLS.1/Global Failure with preservation of secure state

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

FPT_TST.1/Global TSF testing

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

- **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/Global The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

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

FPT_PHP.3/Global Resistance to physical attack

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

9.1.2 Product configuration SFR

This chapter covers the Manufacturing and Personalization SFR. It also includes additional SFR for the compliance to Note 6.

9.1.2.1 SFR for additional code

FAU_STG.2/MP_Add_code Guarantees of audit data availability

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

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

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

Application Note:

Additional code code is loaded with its integrity information. This integrity information is verified by the TOE after the loading, and before the writing of the identification information by calculating the

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

signature and comparing to the expected value. The signature is protected in integrity through the TOE life cycle, at each power on, the card verifies the integrity of this signature.

FCS_CKM.1/MP_Add_code Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Calculation of LSK_LOAD, from initial LSK and derivation data entered - AES 128 ECB	**128**	**None**

FCS_COP.1/MP_ENC_Add_code Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Encryption of the additional code (ciphered with LSK_LOAD) and signature verification	**AES**	**128**	**[R34]**

FCS_COP.1/MP_MAC_Add_code Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging with BAC - 3DES	**3DES Retail MAC**	**112**	**[R34]**
Secure Messaging with BAC - AES	**AES CMAC**	**128, 192 or 256**	**[R34]**

FDP_UIT.1/MP_Add_code Data exchange integrity

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

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

Application Note

Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the additional code to be installed on the card to be different from the one sent by the TOE Developer.

This SFR control integrity of data import in phase 5, including the additional code but not only.

FMT_MTD.1/MP_Add_code Management of TSF data

FMT_MTD.1.1/MP_Add_code The TSF shall restrict the ability to **[selection** the **[list of TSF data]** to **[authorized identified roles]:**

	List of TSF data	Authorised role
Activate	**Additional code**	**TOE developer**

Application note

The Activation of the additional code modify the TOE. This additional code is ciphered with the LSK_LOAD (LSK and Derivation Data) and activated after the authentication of the TOE developer.

FMT_MTD.1/MP_KEY_READ_Add_code Management of TSF data

FMT_MTD.1.1/MP_KEY_READ_Add_code The TSF shall restrict the ability to **read** the **[data]** to **[authorized identified roles]:**

TSF Data	Authorized Identified roles
LSK	**None**

FMT_SMR.1/MP_Add_code Security roles

FMT_SMR.1.1/MP_Add_code The TSF shall maintain the roles
1. TOE developper

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

FPT_EMS.1/MP_Add_code TOE Emanation

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

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

FTP_ITC.1/MP_Add_code Inter-TSF trusted channel

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

FTP_ITC.1.2/MP_Add_code [Editorially Refined] The TSF shall permit **the TOE Developer and Prepersonalizer** to initiate communication via the trusted channel.

FTP_ITC.1.3/MP_Add_code The TSF shall initiate communication via the trusted channel for:
1. Additional code loading

9.1.2.2 Manufacturing and Personalization

FCS_CKM.1/MP Cryptographic key generation

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Cryptographic key generation algorithm	Key length (bits)	Standards
MSK derivation from initial MSK loaded in phase 1 using SHA 256	256	None

FCS_COP.1/MP_ENC_3DES Cryptographic operation

FCS_COP.1.1/MP_ENC_3DES The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following **[standard]**:

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging – encryption and decryption	3DES in CBC mode	112	[R31]

FCS_COP.1/MP_ENC_AES Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging – encryption and decryption	AES in CBC mode	128, 192 and 256	[R34]

FCS_COP.1/MP_MAC_3DES Cryptographic operation

FCS_COP.1.1/MP_MAC_3DES The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following **[standard]**:

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging – MAC	3DES RMAC	112	[R31]

FCS_COP.1/MP_MAC_AES Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging MAC	**AES**	**128, 192 and 256**	**[R34]**

FCS_COP.1/MP_AUTH_3DES Cryptographic operation

FCS_COP.1.1/MP_AUTH_3DES The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following **[standard]**:

Cryptographic operation	Algo	Key length (bits)	Standard
Card Manufacturer Authentication (MSK)	**3DES**	**112**	**[R31]**

FCS_COP.1/MP_AUTH_AES Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Card Manufacturer Authentication (MSK)	**AES**	**128, 192 and 256**	**[R34]**

FCS_COP.1/MP_SHA Cryptographic operation

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

Cryptographic operation	Algo	Key length (bits)	Standard
Hashing	**SHA256**	**None**	**[R26]**

FDP_ACC.2/MP Complete access control

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

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

Application Note
This SFR enforces access control over all the operation performed in phase 5, including additional code loading but not only.

FDP_ACF.1/MP Security attribute based access control

FDP_ACF.1.1/MP The TSF shall enforce the **Prepersonalization Access Control** to objects based on the following **Prepersonalizer Authentication (AS_AUTH_MSK_STATUS)**.

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

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

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

Application Note
This SFR enforces access control over all the operation in phase 5, including additional code loading but not only.

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

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

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

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

Application Note
This SFR control import of data in phase 5, including the additional code but not only.
This SFR ensures also the MSK diviersification, which is performs once, at first command, without any security requirements preliminary to this action.

FDP_UCT.1/MP Basic data exchange confidentiality

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

Application note
For the Additional code loading access control, the LSK_LOAD is used to cipher the data transmitted.
This SFR control confidentiality of data import in phase 5, including the additional code but not only.

FDP_UIT.1/MP Data exchange integrity

FDP_UIT.1.1/MP The TSF shall enforce the **Prepersonalization Access Control SFP** to **receive** user data in a manner protected from **modification** errors

FDP_UIT.1.2/MP [Editorially refined] The TSF shall be able to determine on receipt of user data, whether **modification of some pieces of the application sent by the Prepersonalizer** has occurred

FIA_AFL.1/MP Authentication failure handling

FIA_AFL.1.1/MP The TSF shall detect when **3** unsuccessful authentication attempts occur related to **authentication of**

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1. Prepersonalizer

FIA_AFL.1.2/MP When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **forbid any authentication attempt as Personalizer**.

FIA_UAU.1/MP Timing of authentication

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

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

FIA_UID.1/MP Timing of identification

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

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

FIA_UAU.4/MP_3DES Single-use authentication mechanisms

FIA_UAU.4.1/MP_3DES The TSF shall prevent reuse of authentication data related to
1. Authentication Mechanisms based on 3DES

FIA_UAU.4/MP_AES Single-use authentication mechanisms

FIA_UAU.4.1/MP_AES The TSF shall prevent reuse of authentication data related to
1. Authentication Mechanisms based on AES

FIA_UAU.5/MP_3DES Multiple authentication mechanisms

FIA_UAU.5.1/MP_3DES The TSF shall provide
1. Symmetric Authentication Mechanism based on 3DES
to support user authentication.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

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

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

FIA_UAU.5/MP_AES Multiple authentication mechanisms

FIA_UAU.5.1/MP_AES The TSF shall provide

1. Symmetric Authentication Mechanism based on AES

to support user authentication.

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

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

FMT_MTD.1/MP Management of TSF data

FMT_MTD.1.1/MP The TSF shall **restrict** the ability **to switch** the **TOE life cycle from phase 5 to phase 6** to **the Prepersonalizer**.

FTP_ITC.1/MP Inter-TSF trusted channel

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

FTP_ITC.1.2/MP [Editorially Refined] The TSF shall permit **the Prepersonalizer** to initiate communication via the trusted channel.

FTP_ITC.1.3/MP The TSF shall initiate communication via the trusted channel for:

1. Personalization Agent key storage

2. Life cycle transition from Prepersonalization to Personalization phase

FMT_MTD.1/MP_INI_ENA 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**.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FMT_MTD.1/MP_INI_DIS Management of TSF data

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/MP_KEY_READ Management of TSF data

FMT_MTD.1.1/MP_KEY_READ The TSF shall restrict the ability to **read** the **[data]** to **[authorized identified roles]:**

TSF Data	Authorized Identified roles
MSK	**None**
Personalization Agent Keys	**None**

FMT_MTD.1/MP_KEY_WRITE Management of TSF data

FMT_MTD.1.1/MP_KEY_WRITE The TSF shall restrict the ability to **write** the **[data]** to **[authorized identified roles]:**

TSF Data	Authorized Identified roles
MSK	**IC manufacturer (created by the developer)**
Personalization Agent Keys	**None**

FAU_SAS.1/MP 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.

FMT_SMF.1/MP 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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

FMT_SMR.1/MP Security roles

FMT_SMR.1.1/MP The TSF shall maintain the roles

1. Manufacturer

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

FPT_EMS.1/MP TOE Emanation

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

1. Prepersonalizer Key

2. Personalization Agent Key

3. MSK

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

1. Prepersonalizer Key

2. Personalization Agent Key

3. MSK

9.1.3 Active Authentication SFR

FCS_COP.1/AA_DSA Cryptographic operation

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

Operation	Algorithm	Key length (bits)	Standard
Digital Signature Creation	**RSA signature (CRT or SFM) with SHA1, 224, 256, 384, 512**	**1024 to 4096 with a step of 256 bits**	**[R24]**

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com

FCS_COP.1/AA_ECDSA Cryptographic operation

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

Operation	Algo	Key length (bits)	Standard
Digital Signature Creation	**ECDSA with SHA1, 224, 256, 384, 512**	**192 to 521 over prime field curves**	**[R24] [R25] [R26] [R27]**

FDP_DAU.1/AA Basic Data Authentication

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

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

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

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

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

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

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

FMT_MTD.1/AA_KEY_READ Management of TSF data

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FPT_EMS.1/AA TOE Emanation

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

1. Active Authentication: Private Key (AAK)

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

1. Active Authentication: Private Key (AAK)

FMT_MOF.1/AA Management of security functions behaviour

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

FMT_MTD.1/AA_KEY_WRITE Management of TSF data

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

9.1.4 Chip Authentication SFR

FIA_API.1/CA Authentication Proof of Identity

FIA_API.1.1/CA The TSF shall provide a **Chip Authentication protocol according to [R38]** to prove the identity of the **TOE**.

FCS_CKM.1/CA_DH_SM_3DES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	**112**	**[R2]**

FCS_CKM.1/CA_DH_SM_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on the Key Diffie-Hellman key derivation protocol compliant to PKCS#3	**128, 192, 256**	**[R2]**

FCS_CKM.1/CA_ECDH_SM_3DES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	**112**	**[R2]**

FCS_CKM.1/CA_ECDH_SM_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
Algorithm based on ECDH key derivation protocol compliant to ISO 15946	**128, 192, 256**	**[R2]**

FCS_COP.1/CA_SHA_SM_3DES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
SHA1	None	[R26]

FCS_COP.1/CA_SHA_SM_AES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
SHA1 and SHA256	None	[R26]

FCS_COP.1/CA_SYM_SM_3DES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
3DES CBC mode	112	[R26]

FCS_COP.1/CA_SYM_SM_AES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
AES	128, 192 and 256	[R26]

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1/CA_MAC_SM_3DES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
3DES Retail MAC	**112**	**[R38]**

FCS_COP.1/CA_MAC_SM_AES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
AES CMAC	**128, 192 and 256**	**[R38]**

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

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

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

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

FIA_UAU.1/CA Timing of authentication

FIA_UAU.1.1/CA The TSF shall allow:

1. To establish the communication channel

2. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

3. To identify themselves by selection of the authentication key

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4. To carry out the Chip Authentication Protocol
on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.5/CA_3DES Multiple authentication mechanisms

FIA_UAU.5.1/CA_3DES The TSF shall provide
1. Secure Messaging in MAC-ENC mode
2. Symmetric Authentication Mechanism based on 3DES
to support user authentication.

FIA_UAU.5.2/CA_3DES The TSF shall authenticate any user's claimed identity according to the
1. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism

FIA_UAU.5/CA_AES Multiple authentication mechanisms

FIA_UAU.5.1/CA_AES The TSF shall provide
1. Secure Messaging in MAC-ENC mode
2. Symmetric Authentication Mechanism based on AES
to support user authentication.

FIA_UAU.5.2/CA_AES The TSF shall authenticate any user's claimed identity according to the
1. After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism

FIA_UAU.6/CA Re-authenticating

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

FIA_UID.1/CA Timing of identification

FIA_UID.1.1/CA The TSF shall allow
1. To establish the communication channel
2. To read the Initialization Data if it is not disbled by TSF according to FMT_MTD.1/INI_DIS
3. To carry out th Chip Authentication Protocol
on behalf of the user to be performed before the user is identified.

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

FPT_EMS.1/CA TOE Emanation

FPT_EMS.1.1/CA The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to
1. Chip Authentication: Session Keys, Private Key (CAK)

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

FPT_TST.1/CA TSF testing

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

- **When performing the Chip Authentication**

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

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

FMT_MTD.1/CA_KEY_WRITE Management of TSF data

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

FMT_MTD.1/CA_KEY_READ Management of TSF data

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

FDP_UCT.1/CA Basic data exchange confidentiality

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

FDP_UIT.1/CA Data exchange integrity

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

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

9.1.5 PACE SFR

FCS_CKM.1/ECDH_PACE_3DES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
DH key derivation protocol compliant to PKCS#3	**3DES 2 keys**	**[R2]**

FCS_CKM.1/ECDH_PACE_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
DH key derivation protocol compliant to ISO 15946	**128, 192 & 256**	**[R2]**

FCS_CKM.1/DH_PACE_3DES Cryptographic key generation

FCS_CKM.1.1/DH_PACE_3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[cryptographic key generation algorithm]** and specified cryptographic key sizes **[key length]** that meet the following **[standard]**:

Cryptographic key generation algorithm	Key length (bits)	Standards
DH key derivation protocol compliant to PKCS#3	**3DES 2 keys**	**[R2]**

FCS_CKM.1/DH_PACE_AES Cryptographic key generation

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

Cryptographic key generation algorithm	Key length (bits)	Standards
DH key derivation protocol compliant to ISO 15946	**128, 192 & 256**	**[R2]**

FCS_COP.1/PACE_ENC_AES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
AES in CBC mode	**128, 192 and 256**	**[R34]**

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1/PACE_ENC_3DES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
3DES in CBC mode	**112**	**[R31]**

FCS_COP.1/PACE_MAC_AES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
CMAC AES	**128, 192 and 256**	**[R34]**

FCS_COP.1/PACE_MAC_3DES Cryptographic key generation

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

Cryptographic algorithm	Key length (bits)	Standards
Retail MAC with 3DES	**112**	**[R31]**

FDP_ACC.1/TRM Complete access control

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ACF.1/TRM Security attribute based access control

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

1. Subjects:

a. Terminal

b. BIS-PACE

2. Objects:

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

b. Data in EF.DG3 of the logical MRTD

c. Data in EF.DG4 of the logical MRTD

d. All TOE intrinsic secret cryptographic keys stored in the travel document

3. Security attributes:

a. Authentication status of terminals

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

1. A BIS-PACE is allowed to read data objects from FDP.ACF.1.1/TRM according to [R2] after a successful PACE authentication a required by FIA_UAU.1/PACE

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

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document

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

FDP_RIP.1 Subset residual information protection

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

1. Session Keys (immediately after closing related communication session)

2. The ephemeral private key ephem-SK$_{PICC}$- PACE (by having generated a DH shared secret)

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD

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

FDP_UIT.1/TRM Data exchange integrity

FDP_UIT.1.1/TRM The TSF shall enforce the **Access Control SFP** to be able to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors

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

FIA_AFL.1/PACE Authentication failure handling

FIA_AFL.1.1/PACE The TSF shall detect when **an administrator configurable positive integer within range of acceptable values 0 to 255 consecutive** unsuccessful authentication attempts occur related to **authentication attempts using the PACE password as shared password**

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

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

1. To establish the communication channel

2. Carrying out the PACE Protocol according to [4]

3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

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

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

FIA_UAU.4/PACE Single-use authentication mechanisms

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

1. PACE Protocol according to [4]

2. Authentication Mechanisms based on Triple-DES and AES

FIA_UAU.5/PACE Multiple authentication mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE Protocol according to [R2]

2. Passive Authentication according to [R3]

3. Secure messaging in MAC-ENC mode according to [R2]

to support user authentication.

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

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol

FIA_UAU.6/PACE Re-authenticating

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

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

1. To establish the communication channel

2. Carrying out the PACE Protocol according to [4]

3. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

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

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FMT_MTD.1/PACE_KEY_READ Management of TSF data

FMT_MTD.1.1/PACE_KEY_READ The TSF shall restrict the ability to **read** the
1. PACE passwords
to **none**.

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles
1. Terminal
2. PACE authenticated BIS-PACE

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

FPT_EMS.1/PACE TOE Emanation

FPT_EMS.1.1/PACE The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to
1. PACE: Session Keys (PACE-KMAC, PACE-KENC), Ephemeral Private Key ephem SKPICC-PACE

FPT_EMS.1.2/PACE The TSF shall ensure any **unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to
1. PACE: Session Keys (PACE-KMAC, PACE-KENC), Ephemeral Private Key ephem SKPICC-PACE

FTP_ITC.1/PACE Inter-TSF trusted channel

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

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

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

FPT_TST.1/PACE TSF testing

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

- **When performing a PACE authentication**

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

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

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

FMT_MTD.1/PA Management of TSF data

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

9.1.6 PACE CAM SFR

FIA_UAU.1/PACE_CAM Timing of authentication

FIA_UAU.1.1/PACE_CAM The TSF shall allow

1. Carrying out the PACE Protocol according to [4]

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

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

FIA_UAU.4/PACE_CAM Single-use authentication mechanisms

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

Aditionally to FIA_UAU.4/PACE

1. PACE CAM Protocol according to [4]

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

FIA_UAU.5/PACE_CAM Multiple authentication mechanisms

FIA_UAU.5.1/PACE_CAM The TSF shall provide
1. PACE CAM Protocol according to [4]
to support user authentication.

FIA_UAU.5.2/PACE_CAM The TSF shall authenticate any user's claimed identity according to the **following rules:**
The same rules from FIA_UAU.5.2/PACE applies, with the PACE_CAM protocol

FIA_UAU.6/PACE_CAM Re-authenticating

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

FIA_UID.1/PACE_CAM Timing of identification

FIA_UID.1.1/PACE_CAM The TSF shall allow additionally to FIA_UID.1/PACE:
1. Carrying out the PACE CAM Protocol according to [4]
on behalf of the user to be performed before the user is identified.

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

FMT_MTD.1/PACE_CAM_KEY_READ Management of TSF data

FMT_MTD.1.1/PACE_CAM_KEY_READ The TSF shall restrict the ability to **read** the
1. PACE passwords
2. PACE CAM Private Key
to **none**.

FMT_MTD.1/PACE_CAM_KEY_WRITE Management of TSF data

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

9.2 Security Assurance Requirements

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

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves -
92700 Colombes - France I info@oberthur.com

10 TOE SUMMARY SPECIFICATION

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

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

- PACE keys
- PACE CAM keys
- Chip Authentication keys
- Active Authentication private key
- Personalization Agent keys
- MSK and LSK
- CVCA keys

It controls access to the CPLC data as well:

- It ensures the CPLC data can be read during the personalization phase
- It ensures it can not 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), the Document Security Object, EF.CVA, 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 throught 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)

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

Access Control in writing

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

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

It ensures as well the CPLC data can not be written anymore once the TOE is personalized and that it is not possible to load an additional code.

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 [R38]

In the 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).

Active Authentication

This security functionality ensures the Active Authentication is performed as described in **[R38]**. (if it is activated by the personnalizer).

Chip Authentication

This security functionality ensures the Chip Authentication is performed as described in **[R38]** (if it is activated by the personnalizer). It could be used as an alternative of Active Authentication to reinforce the Authentication of the Chip. It differs from an EAC not performing the Terminal Authentication.

PACE mechanism

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

PACE_CAM mechanism

This security functionality ensures the PACE_CAM is correctly performed. It can only be performed once the TOE is personalized with :

- the chip authentication mapping (CAM) keys the Personnalization Agent loaded during the personalization phase
- the PACE password.

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

Personalization

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

Authentication mechanism based on a Triple DES or AES algorithm. This TSF can use a Secure Messaging described in the TSF Secure Messaging.

Physical protection

This security functionality protects the TOE against physical attacks.

Prepersonalization

This security functionality ensures the TOE, when delivered to the Prepersonnalization Agent, demands an authentication prior to any data exchange. This authentication is based on a symmetric Authentication mechanism based on a Triple DES or AES algorithm. This function is in charge of pre-initializing the product and loading additional code if needed. This TSF is conformant with **[R44]**. 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 EEPROM)

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

Secure Messaging

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

After a successful PACE authentication and successful Chip Authentication, a secure channel is established based on Triple DES algorithm, and after a successful Chip Authentication , a secure channel is (re)established based on Symetric algorithms (Triple DES, AES128, 192 or 256)

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 PACE or EAC)

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

This Secure Messaging can be combined with the Active Authentication.

This TSF can provide a GP Secure Messaging (SCP02 or SCP03) for the Prepersonalization or Personalization.

Self tests

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

- Before the TSF data usage
- The additional code integrity is checked at each POWER ON of the card
- The integrity of keys and sensitive data is ensured

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

11 RATIONALES

Threats	Security Objectives
T.Skimming	OT.Data_Int, OT.Data_Auth, OT.Data_Conf, OT.MRTD_Holder
T.Eavesdropping	OT.Data_Conf
T.Tracing	OT.Tracing, OE.MRTD_Holder
T.Forgery	OT.AC_Pers, OE.Personalization, OT.Data_Int, OT.Data_Auth, OT.Prot_Phys-Tamper, OT.Prot_Abuse-Func, OE.Terminal, OE.Pass_Auth_Sign, OE.Exam_MRTD_AA
T.Abuse-Func	OT.Prot_Abuse-Func, OE.Personalization
T.Information_Leakage	OT.Prot_Inf_Leak
T.Phys-Tamper	OT.Prot_Phys-Tamper
T.Malfunction	OT.Prot_Malfunction
T.Counterfeit	OT.CA_Proof, OT.Data_Int_CA, OE.Terminal, OT.AA_Proof, OT.Data_Int_AA, OE.Activ_Auth_Verif
T.Unauthorized_Load	OT.Secure_Load_ACode
T.Bad_Activation	OT.Secure_AC_Activation
T.TOE_Identification_Forgery	OT.TOE_Identification

Table 11- Threats and Security Objectives – coverage

OSP	Security Objectives
P.Manufact	OT.Identification
P.Pre_operational	OT.Identification, OT.AC_Pers, OE.Personalization, OE.Legislative_Compliance
P.Card_PKI	OE.Passive_Auth_Sign
P.Trustworthy_PKI	OE.Passive_Auth_Sign
P.Terminal	OE.Terminal
P.Activ_Auth	OT.AA_Proof
P.Chip_Auth	OT.CA_Proof

Table 12 - OSPs and Security Objectives – Coverage

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

Table 13 - Assumptions and OE – Coverage

The other rationales are available in the complete ST.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

12 REFERENCES

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 – v1.11

[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

IDL specifications

[R7] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 1:Physical characteristics and basic data set, ISO/IEC 18013-1:2005

[R8] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 2: Machine-readable technologies, ISO/IEC 18013-2:2008

[R9] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 3: Access control, authentication and integrity validation, ISO/IEC 18013-3:2009

Protection Profiles

[R10] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0035 15/06/2007

[R11] Machine readable travel documents with "ICAO Application", Basic Access control – BSI-PP-0055 v1.10 25th march 2009

[R12] Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009

[R13] Machine readable travel documents with "ICAO Application", Extended Access Control with PACE (EAC PP) – BSI-PP-0056 V2 – 2012

[R14] MRTD with PACE – PP-0068v2

[R15] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007

[R16] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009

[R17] Technical Report, Supplemental Access Control for Machine Readable Travel Documents – version v1.01

Chips References

[R18] Certification report - BSI-DSZ-CC-0978-2016 - NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC dedicated software

Standards

[R19] ISO/IEC 7816-4:2013 – Organization, security and commands for interchange

[R20] Technical Guideline: Elliptic Curve Cryptography according to ISO/IEC 15946.TR-ECC, BSI 2006

[R21] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[R22] ISO/IEC 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[R23] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[R24] ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function

[R25] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993

[R26] 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

[R27] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 septembre 1998

[R28] Jakob Jonsson and Burt Kaliski. Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1. RFC 3447, 2003

[R29] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002

[R30] ANSI X9.31 - Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[R31] FIPS 46-3 Data Encryption Standard (DES)

[R32] ISO/IEC 9797-1:1999 "Codes d'authentification de message (MAC) Partie 1: Mécanismes utilisant un cryptogramme bloc"

[R33] NIST SP 800-90 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)

[R34] FIPS 197 – Advance Encryption Standard (AES)

[R35] ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Misc

[R36] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R37] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

[R38] Advanced Security Mechanisms for Machine Readable Travel Documents part 1 – Technical Guideline TR-03110-1 – version 2.10 March 2012

[R39] Advanced Security Mechanisms for Machine Readable Travel Documents part 2 – Technical Guideline TR-03110-2 – version 2.10 March 2012

[R40] Advanced Security Mechanisms for Machine Readable Travel Documents part 3 – Technical Guideline TR-03110-3 – version 2.10 March 2012

CC

[R41] 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

[R42] Common Criteria for Information Technology security Evaluation Part 2: Security Functional Components, CCMB-2012-09-002, version 3.1 Revision 4 Final, September 2012

[R43] Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Components, CCMB-2012-09-003, version 3.1 Revision 4 Final, September 2012

[R44] ANSSI-CC note 6 – v0.91

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com

S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

13 ACRONYMS

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

INDEX

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534