ID-One eIDL v1.0 in EAC configuration with BAP and AA on NXP P60x144 PVA/PVE

Public Security Target
FQR No: 110 8165
FQR Issue: 1

[redacted]

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 eIDL v1.0 in EAC configuration with BAP and AA on NXP P60x144 PVA/PVE
FQR No:	110 8165
FQR Issue:	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

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

List of Figures

List of tables

1 SECURITY TARGET INTRODUCTION

1.1 Purpose

The objective of this document is to present the Public Security Target of ID-One eIDL v1.0 in EAC configuration with BAP and AA on NXP P60x144 PVA/PVE.

1.2 Objective of the security target

This security target describes the security needs for ID-One eIDL v1.0 product. The product is based on PP EAC 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 eIDL v1.0 in EAC configuration with BAP and AA 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-056 [R12]
ST Reference:	FQR 110 7894 Issue 2
ITSEF:	LETI
Certification Body:	ANSSI
Evaluation scheme:	FR

Table 1 - General Identification

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

1.4 TOE technical identification

Product name:	ID-One ePass Full EAC v2
Commercial name of the TOE:	ID-One eIDL v1.0 in EAC configuration with BAP and AA on NXP P60x144 PVA/PVE
IC type	'6A15' (P60D144 VA) '6A20' (P60C144 VA) '6E15' (P60D144 VE) '6E20' (P60C144 VE)
Additional code 1 Mandatory generic Identification:	'082456FF412E4D1EC087005B56A9A2CAC0B6558F4CAAE041D8B5A69345559B562A6F4C8E'
Additional code 2 Optional DBI Identification:	'082844FFE339C30BC6A81162413612FE2698284FA6CD28AA5CF5257A20B83611E58E9BEE'
Guidance documents	MINOS - ID-One eIDL v1.0 in EAC configuration with BAP and AA - Guidance Document - PREparative procedures FQR 110 7931 Issue 2 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 + ALC_FLR.1
Communication protocol:	Contact, Contactless and Dual
Memory:	ROM
Chip Manufacturer:	NXP Semiconductors

Table 3 - Chip Identification

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 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:

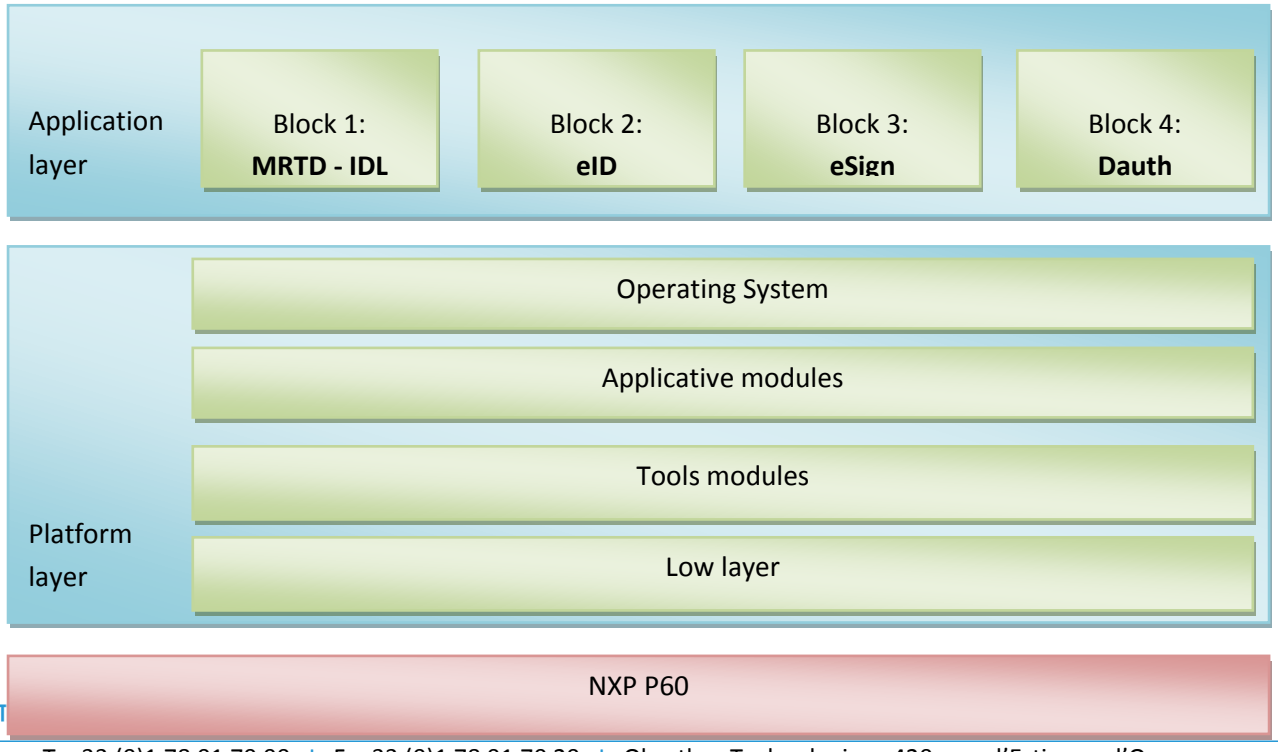

Figure 1 - ID-One Native eDoc Overview

2.2 TOE overview

The TOE described in this security target is the EAC with BAP 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
PACE and EAC	X	EAL5 + ALC_DVS.2 + AVA_VAN.5

Table 4 - Block 1 Applications overview

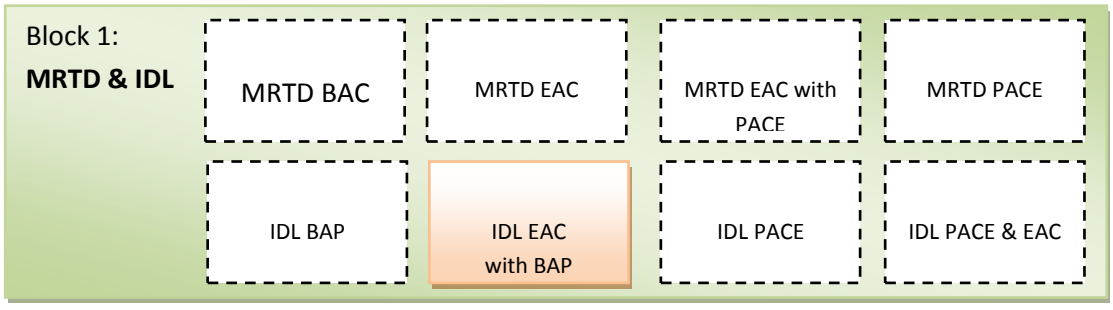

Figure 2 - Block 1 Overview

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 EAC with BAP TOE is instantiated during the product prepersonalization, using the operating system that creates the MF / DF required for the EAC with BAP 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:

- Extended Access Control with Chip Authentication and Terminal Authentication
- Basic Access Protection
- Active Authentication
- Prepersonalization phase (in particular with Additional code loading)
- Personalization phase

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

Organisation issues MRDs 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 MRD 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 MRD 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 MRD in context of this security target contains:

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

The authentication of the holder is based on:

- The possession of a valid MRD personalized for a holder with the claimed identity as given on the biographical data page and

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 Biometric matching performed on the Inspection system using the reference data stored in the MRD.

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

The issuing Organization ensures the authenticity of the data of genuine MRDs. The receiving Organization trusts a genuine MRD of an issuing Organization.

The MRD can be viewed as the combination:

- **A physical MRD** 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 MRD holder
  - The biographical data on the biographical data page of the Driving Licence Document
  - The printed data in the Machine-Readable Zone (keydoc)keydoc area that identifies the device
  - The printed portrait
- **A logical MRD** as data of the MRD 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 MRD holder
  - The digital Machine Readable Zone Data (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 toDG64)
  - The Document security object

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

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

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

2.4 TOE definition

The Target of Evaluation (TOE) is the contact, contactless and dual integrated circuit chip of machine readable documents (MRD's chip) programmed according to the Logical Data Structure (LDS) and providing the following features:

- Basic Access Protection
- Active Authentication
- Extended Access Control

The TOE comprises at least:

- Circuitry of the MRD'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)
- MRD application
- Associated guidance documentation

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 OE ARCHITECTURE

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

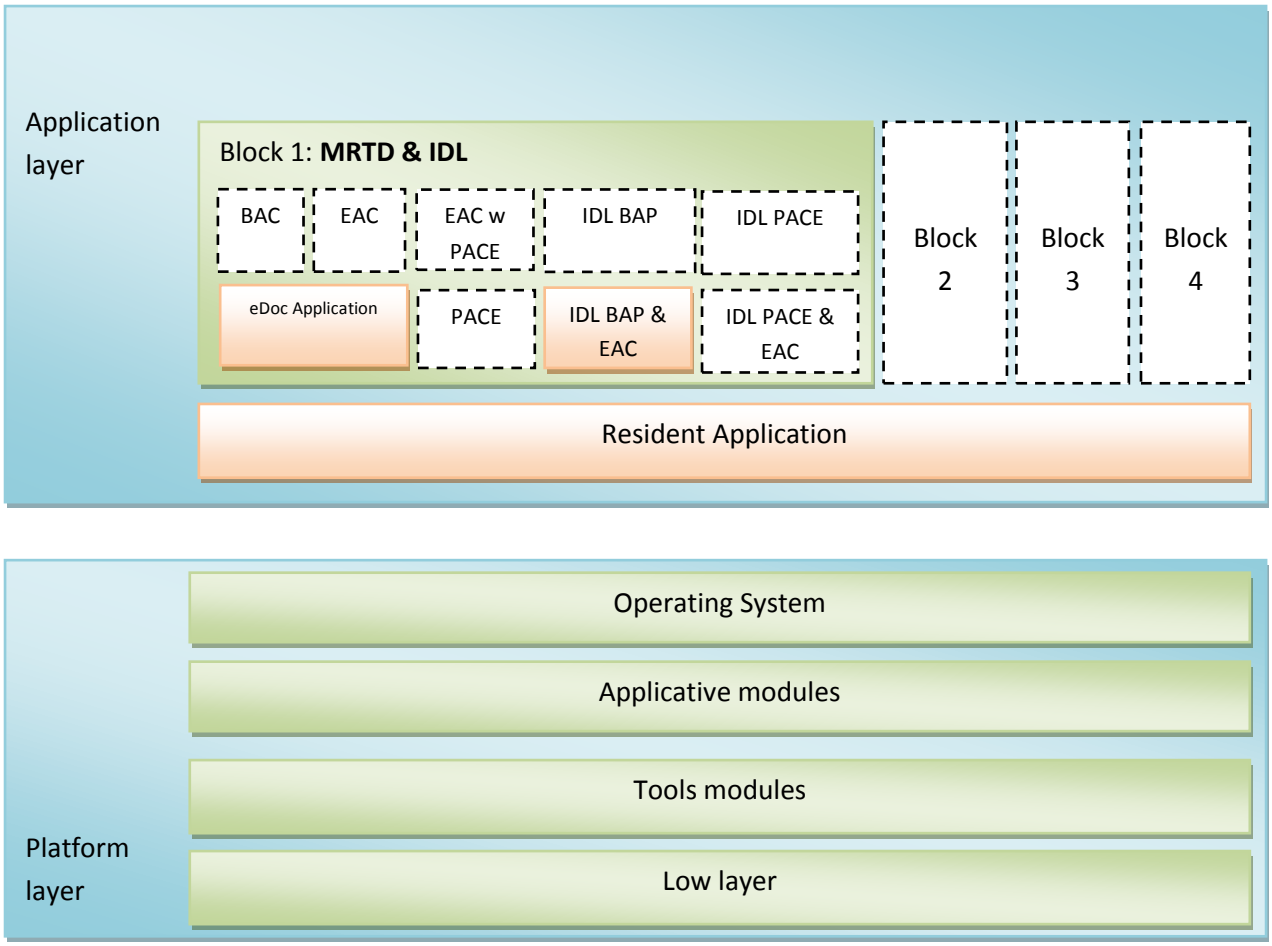

Figure 3 - TOE architecture

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.

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 IDL 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 IDL 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 IDL 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 IDL 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 MRD Applications.

The application layer also manages protocols available during Use phase such as Basic Access Control, Basic Access Protection, Extended Access Control or Active Authentication.

The protocol for Basic Access Control is specified by ICAO **[R2]**. Basic Access Control checks that the terminal has physical access to the MRD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read KEYDOC of the MRD. 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 KEYDOC (for MRD),
- Authenticates itself as inspection system by means of keys derived from KEYDOC 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 Basic Access Protection (BAP) is especially used in the context of IDL as an alternative to BAC. Indeed it is actually a generalisation of BAC allowing usage of extra algorithms and key length. It exists in 4 modes:
BAP1 - 3DES with key length of 128 bits (equivalent to BAC),
BAP2 - AES with key length of 128 bits,
BAP3 - AES with key length of 192 bits,
BAP4 - AES with key length of 256 bits.
Following Secure messaging is performed using the algorithm used in the selected BAP mode.

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

Note that the term MRZ is specific to ICAO standard; [R8] uses the term “Keydoc” which refers to an equivalent unique identifier printed on the physical TOE as a random number or barcode.

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 DG7 and DG8. 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 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 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.

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 TOE LIFE CYCLE

4.1 Life cycle overview

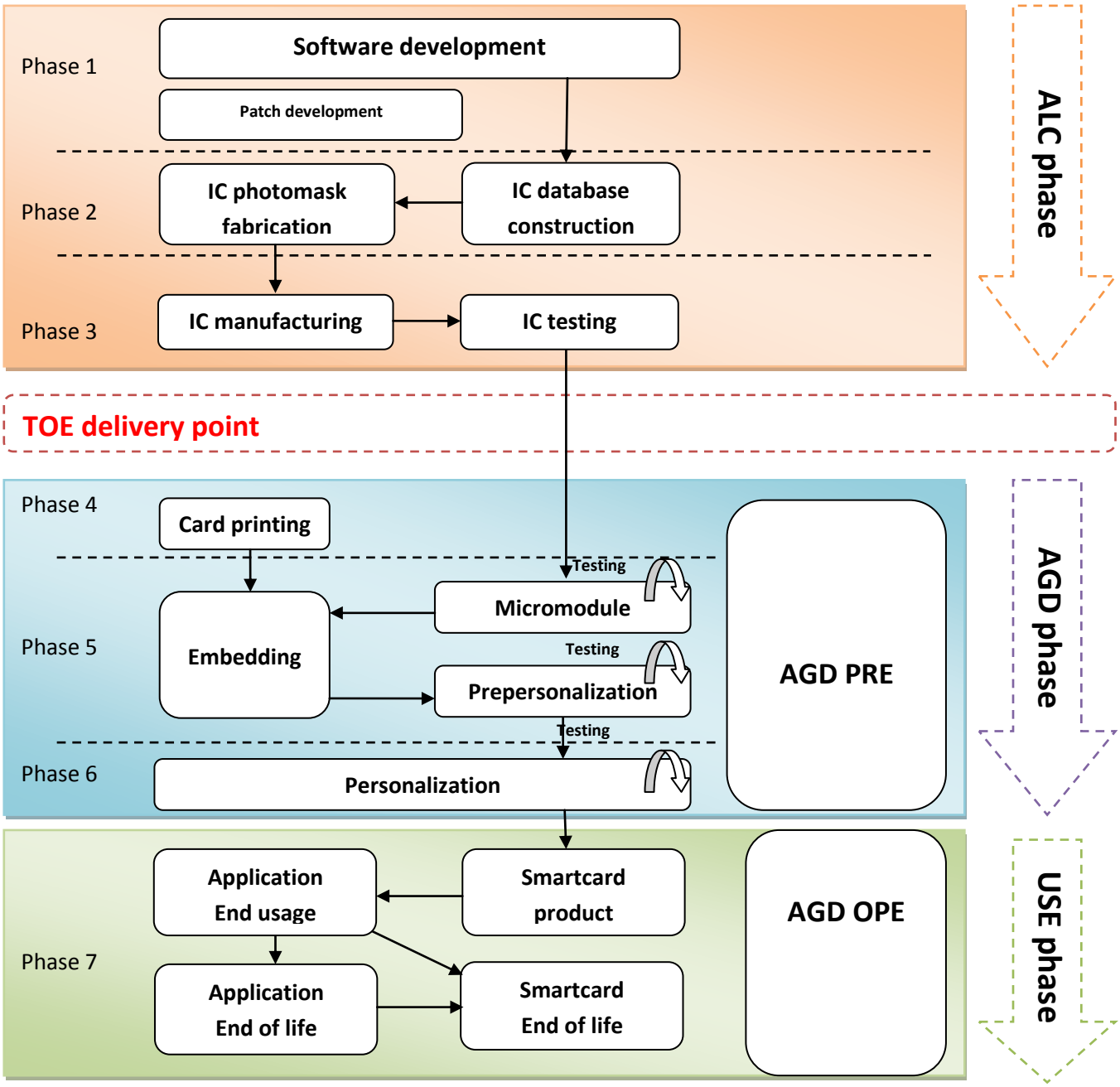

Figure 4: Smartcard product life-cycle for the TOE

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 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

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

4.2 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 IDL 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 eIDL 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 document's chip Dedicated Software and the parts of the 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 eIDL application, and (iii) equips travel document's chips with pre-personalization 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 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 MRD 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 KEYDOC data (EF.DG1), (ii) the digitized portrait (EF.DG6), 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 Organisation and can be used according to the security policy of the issuing Organization but they can never be modified.

Note that the personalization process and its environment may depend on specific security needs of an issuing 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.

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

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 (/CA) that are dedicated for Chip Authentication
- SFR (/TA) that are dedicated for Terminal Authentication
- SFR (/BAC and /BAP) that are dedicated for Basic Access Protection
- SFR (/EAC) that are dedicated for Extended Access Control

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

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

SFR from the PP
FAU_SAS.1; FCS_CKM.1; FCS_CKM.4; FCS_COP.1/SHA ; FCS_COP.1/SYM ; FCS_COP.1/MAC ; FCS_COP.1/SIG_VER ; FCS_RND.1; FIA_UID.1; FIA_UAU.1; FIA_UAU.4 ; FIA_UAU.5; FIA_UAU.6 ; FIA_API.1 ; FDP_ACC.1 ; FDP_ACF.1 ; FDP_UCT.1 ; FDP_UIT.1 ; FMT_SMF.1; FMT_SMR.1; FMT_LIM.1; FMT_LIM.2 FMT_MTD.1/INI_ENA ; FMT_MTD.1/INI_DIS ; FMT_MTD.1/CVCA_INI ; FMT_MTD.1/CVCA_UPD ; FMT_MTD.1/DATE ; FMT_MTD.1/KEY_WRITE ; FMT_MTD.1/CAPK; FMT_MTD.1/KEY_READ; FMT_MTD.3; 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

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: **§ 6.3.2 Threats for AA**
- Additional Objective: **§ 7.1.2 SO for AA**
- Additional OE: **§ 7.2.2 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: **§ 6.3.3 Threats for Note 6**
- Additional Objective: **§ 7.1.3 SO for Note 6**

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

5.2 Protection Profile conformance

The Security Target is based on the following PP written in CC3.1 revision 2:

- Machine Readable Travel Documents with "ICAO Application", Extended Access Control [R12].

For consistency reasons, editorial modifications have been performed:

- BAC replaced by BAP
- MRTD replaced by MRD
- "DG1 to DG16" replaced by "DG1 to DG24"
- State replaced by organization
- MRZ replaced by keydoc
- Reference to EF.COM for access control rules (which specifies which DG is protected by BAP or EAP)
- DG2 replaced by DG6
- DG3 replaced by DG7
- DG4 replaced by DG8
- DG15 replaced by DG13

5.3 Rationale for the additions

The rationales are available in the complete ST.

5.4 Non evaluated features

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
- PACE
- 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 EAC subjects

Manufacturer

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

Personalization Agent

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

Application Note

Personalization Agent is refered as the Personalizer in the Security Target

Country Verifying Certification Authority

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

Document Verifier

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

Terminal
A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface.

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

MRD Holder
The rightful holder of the MRD for whom the issuing Organization personalized the MRD.

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

Attacker
A threat agent trying (i) to manipulate the logical MRD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG7, EF.DG8) or (iii) to forge a genuine MRD.

Application Note

- Note that an attacker trying to identify and to trace the movement of the MRD's chip remotely (i.e. without knowing or optically reading the physical MRD) is not considered by this PP since this can only be averted by the BAP mechanism using the "weak" Document Basic Access Keys that is covered by [25]. The same holds for the confidentiality of the user data EF.DG1, EF.DG6, EF.DG5 to EF.DG24 as well as EF.SOD and EF.COM.

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

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 MRD manufacturer as described in [R11].

6.2 Assets

Logical MRD data
The logical MRD data consists of the EF.COM, EF.DG1 to EF.DG24 (with different security needs) and the Document Security Object EF.SOD according to LDS [R2]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRD.
The current EAC Security Target is dedicated to the protection of both Active Authentication EF.DG13 (see below) and sensitive biometric EF.DG7&4. The other one (and associated keys) are described and managed in the related BAP Security Target.
The Active Authentication Public Key Info in EF.DG13 is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRD.
All these data may be sorted out in two different categories.
If they are specific to the user, they are User data,
If they ensure the correct behaviour of the application, they are TSF Data.

User Data	Description

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

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	Contain the fingerprint and the iris picture
Active Authentication Public Key in EF.DG13 (AAPK)	Contains public data enabling to authenticate the chip thanks to an Active Authentication
Chip Authentication Public Key in EF.DG14 (CAPK)	Contains public data enabling to authenticate the chip thanks to an the Chip Authentication Protocol

Table 11 - User Data

TSF Data	Description
TOE_ID	Data enabling to identify the TOE
Prepersonalizer reference authentication data	Private key enabling to authenticate the Prepersonalizer
Personalization Agent reference authentication Data	Private key enabling to authenticate the Personalization Agent
Basic Access Control (BAC) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Active Authentication private key (AAK)	Private key the chip uses to perform an Active Authentication
Chip Authentication private key (CAK)	Private key the chip uses to perform a Chip Authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality, authenticity and integrity
Life Cycle State	Life Cycle state of the TOE
Additional Code	Additional code to be loaded on the initial TOE during prepersonalization by the Prepersonalizer. The loading of the additional code on the initial TOE constitures the final 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 12 - TSF Data

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

6.3 Threats

IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

Application note: The threats T.Chip_ID and T.Skimming (cf [R11]) are averted by the mechanisms described in the BAC PP which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRD by identifying remotely the MRD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the KEYDOC or who does not know the physical MRD in advance.

6.3.1 Threats from the PP EAC

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

T.Forgery

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 alters fraudulently the complete stored logical MRD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRD holder"s identity or biometric reference data. This threat comprises several attack scenarios of MRD forgery. The attacker may alter the biographical data on the biographical data page of the Driving Licence book, in the printed KEYDOC and in the digital KEYDOC to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRDs to create a new forged MRD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRD of a traveler into another MRD's chip leaving their digital KEYDOC unchanged to claim the identity of the holder this MRD. The attacker may also copy the complete unchanged logical MRD to another contactless chip.

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

***Asset*:** authenticity of logical MRD data.

T.Counterfeit

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

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

Asset: authenticity of logical MRD data

T.Abuse-Func

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

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

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

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

T.Information_Leakage

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

T.Phys-Tamper
***Adverse action*:** An attacker may perform physical probing of the MRD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRD's chip Embedded Software. An attacker may physically modify the MRD's chip in order to (i) modify security features or functions of the MRD's chip, (ii) modify security functions of the MRD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.
The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.
***Threat agent*:** having enhanced basic attack potential, being in possession of a legitimate MRD.
***Asset*:** confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.

T.Malfunction
***Adverse action*:** An attacker may cause a malfunction of TSF or of the MRD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or

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

functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRD's chip Embedded Software.
This may be achieved e.g. by operating the MRD's chip outside the normal operating conditions, exploiting errors in the MRD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
***Threat agent*:** having enhanced basic attack potential, being in possession of a legitimate MRD.
***Asset*:** confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.

6.3.2 Threats for AA

T.Counterfeit

6.3.3 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 MRD
Asset: Logical MRD data

T.Bad_Activation
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 MRD, being in possession of an additional code that is authorized to be load
Asset: Logical MRD 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 MRD
Asset: TOE_ID

Application Note

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

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 EAC

P.BAC-PP

The issuing Organizations or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRD data DG1, DG6, DG5 to DG24 the "ICAO Doc 9303" [R2] as well as to the data groups Common and Security Data. The MRD is successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "DRIVING LICENCE Application", Basic Access Control" [R11] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRD data.

Application note: The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [R2] is addressed by the [R11] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG7 and EF.DG8 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [R11]). The TOE shall protect the sensitive biometric reference data in EF.DG7 and EF.DG8 against attacks with high attack potential. Due to the different resistance the protection of EF.DG7 and EF.DG8 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG6 and EF.DG5 to EF.DG24 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates.

P.Sensitive_Data

The biometric reference data of finger(s) (EF.DG7) and iris image(s) (EF.DG8) are sensitive private personal data of the MRD holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the MRD is presented to the inspection system (Extended Inspection Systems). The issuing Organization authorizes the Document Verifiers of the receiving Organizations to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The MRD's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

P.Manufact

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

P.Personalization

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

6.4.2 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.

6.5.1 Assumptions from PP EAC

A.MRD_Manufact

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

A.MRD_Delivery

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

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

A.Pers_Agent

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

A.Insp_Sys

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

The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing Organization through the Document Verifier of the receiving Organization to read the sensitive biometric reference data.

A.Signature_PKI

The issuing and receiving Organizations or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRD. The issuing 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 Organizations maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving Organizations and Organizations.

A.Auth_PKI

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

6.5.2 Assumptions for Active Authentication

A.Insp_Sys_AA

The Inspection System implements the Active Authentication Mechanism. The Inspection System verifies the authenticity of the MRD’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 EAC

OT.AC_Pers
The TOE must ensure that the logical MRD data in EF.DG1 to EF.DG24, the Document security object according to LDS [R2] and the TSF data can be written by authorized Personalization Agents only. The logical MRD data in EF.DG1 to EF.DG24 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG24 are added.

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

OT.Sens_Data_Conf
The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG7 and EF.DG8) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing Organization. The TOE must ensure the confidentiality of the logical MRD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Identification
The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRD". The storage of the Pre- Personalization

data includes writing of the Personalization Agent Key(s). The storage of the Prepersonalization data includes writing of the Personalization Agent Key(s).

OT.CA_Proof

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

OT.Prot_Abuse-Func

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

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

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

OT.Prot_Inf_Leak

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

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

OT.Prot_Phys-Tamper

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRD's chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

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

with a prior

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

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

OT.Prot_Malfunction

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

7.1.2 SO for AA

OT.AA_Proof

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

OT.Data_Int_AA

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

7.1.3 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.

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

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 EAC

7.2.1.1 Issuing Organization

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

OE.MRD_Manufact

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

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

OE.MRD_ Delivery

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

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

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

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

OE.Personalization

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

- (i) Establish the correct identity of the holder and create biographical data for the MRD
- (ii) Enroll the biometric reference data of the MRD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s)
- (iii) Personalize the MRD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign

The issuing Organization must:

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

The issuing Organization must:

- (i) Generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys
- (ii) Sign Document Security Objects of genuine MRD in a secure operational environment only
- (iii) Distribute the Certificate of the Document Signer Public Key to receiving Organizations and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG24 if stored in the LDS according to [R2].

OE.Auth_Key_MRD

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

- (i) Generate the MRD'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 Organizations or organizations to verify the authenticity of the MRD's chip used for genuine MRD by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data

The issuing Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRD's holders to authorized receiving Organizations

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

or Organizations. The Country Verifying Certification Authority of the issuing Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.BAC-PP

It has to be ensured by the issuing Organization, that the TOE is additionally successfully evaluated and certified in accordance with the "Common Criteria Protection Profile Machine Readable Travel Document with "DRIVING LICENCE Application", Basic Access Control" [R11]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

7.2.1.2 Receiving Organization

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

OE.Exam_MRD

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

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

OE.Pass_Auth_Verif

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

OE.Prot_Logical_MRD

The inspection system of the receiving Organization ensures the confidentiality and integrity of the data read from the logical MRD. The receiving Organization examining the logical MRD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

OE.Ext_Insp_Systems

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

7.2.2 OE for AA

OE.Exam_MRD_AA

Aditionally to the OE.Exam_MRD, the inspection systems perform the Active Authentication protocol to verify the Authenticity of the presented MRD's chip.

OE.Prot_Logical_MRD_AA

Aditionally to the OE.Prot_Logical_MRD, 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 MRD.

OE.Activ_Auth_Sign

The issuing Organization has to establish the necessary public key infrastructure in order to (i) generate the MRD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG13 and (iii) support inspection systems of receiving Organizations to verify the authenticity of the MRD's chip used for genuine MRD by certification of the Active Authentication Public Key by means of the Document Security Object.

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

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

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
- **BAP SFR** that cover the Basic Access Protection
- **CA SFR** that cover the Chip Authentication Protocol
- **TA SFR** that cover the Terminal Authentication Protocol (note: Terminal Authentication Protocol is only available with the Extended Access Control)
- **EAC SFR** that cover the Extended Access Control (note: EAC protocol is a combination of TA and CA, this chapter only contains SFR that can not be strictly applied to one or another)

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.

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_LIM.1/Global Limited capabilities

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

Deploying Test Features after TOE Delivery does not allow

1. User Data to be manipulated

2. TSF data to be disclosed or manipulated

3. Software to be reconstructed

4. Substantial information about construction of TSF to be gathered which may enable other attacks

FMT_LIM.2/Global Limited availability

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

Deploying Test Features after TOE Delivery does not allow

1. User Data to be manipulated

2. TSF data to be disclosed or manipulated

3. Software to be reconstructed

4. Substantial information about construction of TSF to be gathered which may enable other attacks

FPT_EMS.1/Global TOE Emanation

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

1. EF.COM, EF.SOD and EF.DG1 to EF.DG24

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.DG24

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.

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_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**.

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:
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 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

Cryptographic operation	Algo	Key length (bits)	Standard
Secure Messaging MAC	**3DES Retail MAC**	**112**	**[R34]**
	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

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

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]**:

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]**

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/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]**:

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 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)**.

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.1.3/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.

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_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**
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

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.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.

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**.

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**

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

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

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]**

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.

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

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

FMT_MTD.1/AA_KEY_READ Management of TSF data

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

FPT_EMS.1/AA TOE Emanation

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

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

FMT_MOF.1/AA Management of security functions behaviour

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

FMT_MTD.1/AA_KEY_WRITE Management of TSF data

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

9.1.4 Basic Access Protection SFR

FCS_CKM.1/BAC Cryptographic key generation

FCS_CKM.1.1/BAC 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
Document Basic Access Key Derivation Algorithm	**112**	**[R2]**

FCS_COP.1/BAC_AUTH Cryptographic operation

FCS_COP.1.1/BAC_AUTH 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
Symmetric authentication, encryption and decryption	**3DES**	**112**	**[R34]**

FCS_COP.1/BAC_SHA Cryptographic operation

FCS_COP.1.1/BAC_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	**SHA1**	**None**	**[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/BAC_ENC Cryptographic operation

FCS_COP.1.1/BAC_ENC 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 (BAP) – encryption and decryption	**3DES in CBC mode**	**112**	**[R34][R31]**

FCS_COP.1/BAC_MAC Cryptographic operation

FCS_COP.1.1/BAC_MAC 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	**Retail MAC**	**112**	**[R31]**

FDP_UCT.1/BAC Basic data exchange confidentiality

FDP_UCT.1.1/BAC The TSF shall enforce the **Basic Access Protection SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/BAC Data exchange integrity

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

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

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/BAC_KEY_READ Management of TSF data

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

TSF Data	Authorized Identified roles
Document Access Keys	**None**

FMT_LIM.1/BAC Limited capabilities

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

Deploying Test Features after TOE Delivery does not allow

1. User Data to be disclosed

FMT_LIM.2/BAC Limited availability

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

Deploying Test Features after TOE Delivery does not allow

1. User Data to be disclosed

FPT_TST.1/BAC TSF testing

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

- **When performing a BAPauthentication**

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

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

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/BAC_KEY_WRITE Management of TSF data

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

	List of TSF data	Authorised role
Write	**Document Basic Access Keys**	**Personalization Agent**

FCS_CKM.1/BAP Cryptographic key generation

FCS_CKM.1.1/BAP 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
Document Basic Access Key Derivation Algorithm - AES	**128, 192 and 256**	**[R7]**

FCS_COP.1/BAP Cryptographic operation

FCS_COP.1.1/BAP 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 and decryption	**AES**	**128, 192 and 256**	**[R34]**

FCS_COP.1/BAP-SM Cryptographic operation

FCS_COP.1.1/BAP-SM 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]**:

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 operation	Algo	Key length (bits)	Standard
Secure messaging – message authentication code	**AES in CBC mode**	**128, 192 and 256**	**[R34]**

9.1.5 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]**

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_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	Standards

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

	(bits)	
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]**

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]**

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_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]**

FIA_UAU.1/CA Timing of authentication

FIA_UAU.1.1/CA The TSF shall allow:
1. To establish the communication channel
2. To read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. To identify themselves by selection of the authentication key
4. To carry out the Chip Authentication Protocol
on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.5/CA_3DES Multiple authentication mechanisms

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

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

FIA_UAU.5/CA_AES Multiple authentication mechanisms

FIA_UAU.5.1/CA_AES The TSF shall provide

1. Secure Messaging in MAC-ENC mode
2. Symmetric Authentication Mechanism based on AES
to support user authentication.

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

FIA_UAU.6/CA Re-authenticating

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

FIA_UID.1/CA Timing of identification

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

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

FPT_EMS.1/CA TOE Emanation

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

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

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_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**

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

9.1.6 Terminal Authentication SFR

FCS_COP.1/TA_SHA_RSA Cryptographic key generation

FCS_COP.1.1/TA_SHA_RSA 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, SHA256 and SHA 512	**None**	**[R26]**

FCS_COP.1/TA_SHA_SM_ECC Cryptographic key generation

FCS_COP.1.1/TA_SHA_SM_ECC 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, SHA224, SHA256, SHA384 and SHA512	**None**	**[R26]**

FCS_COP.1/TA_SIG_VER_RSA Cryptographic key generation

FCS_COP.1.1/TA_SIG_VER_RSA The TSF shall perform **digital signature verification** 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
RSA coupled with SHA	**From 1024 to 4096, with a step of 256**	**[R38]**

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/TA_SIG_VER_ECC Cryptographic key generation

FCS_COP.1.1/TA_SIG_VER_ECC The TSF shall perform **digital signature verification** 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
ECC coupled with SHA	**From 192 to 521**	**[R38]**

FIA_UAU.4/TA Single-use authentication mechanisms

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

1. Terminal Authentication Protocol

FMT_MTD.1/TA_CVCA_UPD Management of TSF data

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

1. Country Verifying Certification Authority Public Key

2. Country Verifying Certification Authority Certificate

to **Country Verifying Certification Authority.**

FMT_MTD.1/TA_DATE Management of TSF data

FMT_MTD.1.1/TA_DATE The TSF shall **restrict** the ability **to modify** the **Current Date** to

1. Country Verifying Certification Authority

2. Document Verifier

3. Domestic Extended Inspection System

FPT_TST.1/TA TSF testing

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

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

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

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

FMT_SMR.1/TA Security roles

FMT_SMR.1.1/TA The TSF shall maintain the roles
1. Country Verifying Certification Authority
2. Document Verifier
3. Domestic Extended Inspection System
4. Foreign Extended Inspection System

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

FMT_MTD.1/TA_CVCA_INI Management of TSF data

FMT_MTD.1.1/TA_CVCA_INI The TSF shall **restrict** the ability **to write** the
1. Initial Country Verifying Certification Authority Public Key
2. Initial Country Verifying Certification Authority Certificate
3. Initial Current Date
to **the Personalization Agent**

9.1.7 Extended Access Control SFR

FDP_ACC.1/EAC Subset access control

FDP_ACC.1.1/EAC The TSF shall enforce the **Access Control SFP** on terminals gaining write, read and modification access to data in the **EF.COM, EF.SOD, EF.DG1 to EF.DG24 of the logical MRTD**

FDP_ACF.1/EAC Security attribute based access control

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

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

1. Subjects
- **a. Personalization Agent**
- **b. Extended Inspection System**
- **c. Terminal**

2. Objects
- **a. Data EF.DG1 to EF.DG6 and EF.DG9 to EF.DG24 of the logical MRD**
- **b. Data EF.DG7 and EF.DG8 of the logical MRD**
- **c. Data in EF.COM**
- **d. Data in EF.SOD**

3. Security attributes
- **a. Authentication status of terminals**
- **b. Terminal Authorization**

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

1. The successfully authenticated Personalization Agent is allowed to write and read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG24 of the logical MRD

2. The successfully authenticated EIS with the read access to DG7 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG7 of the logical MRD

3. The successfully authenticated EIS with the read accedd to DG8 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG8 of the logical MRD

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

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

1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG7

2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG8

3. A terminal authenticated as DV is not allowed to read data in the EF.DG7

4. A terminal authenticated as DV is not allowed to read data in the EF.DG8

5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG24 of the logical MRD

6. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG7 to EF.DG8 of the logical MRD

Application Note:

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

Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1 to EF.DG6 and EF.DG9 to EF.DG24 of the logical MRD. According to P.BAC-PP this security features of the MRD are not subject of this protection profile. For more information on the associated DG, please refer to table 3 of the ISO 18013-3.

FMT_MTD.3/EAC Secure TSF data

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

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

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

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

FIA_UAU.5/EAC Multiple authentication mechanisms

FIA_UAU.5.1/EAC The TSF shall provide
1. Terminal Authentication Protocol
2. Secure messaging in MAC-ENC mode
to support user authentication.

FIA_UAU.5.2/EAC The TSF shall authenticate any user's claimed identity according to the
1. 1. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism

FMT_LIM.1/EAC Limited capabilities

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

Deploying Test Features after TOE Delivery does not allow

1. Sensitive User Data (EF.DG7 and EF.DG8) to be disclosed (not available for BAC)

FMT_LIM.2/EAC Limited availability

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

Deploying Test Features after TOE Delivery does not allow

1. User Data to be disclosed

9.2 Security Assurance Requirements

The security assurance requirement level is EAL5 augmented with ALC_DVS.2, and 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:

- BA 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 DG7 & DG8), 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 DG7 & DG8 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)
- The TOE is uniquely identified by a random number, generated at each reset. This unique identifier is called (PUPI)

It ensures as well that no other part of the 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 or change the personalizer authentication keys in personalization phase..

Regarding the file structure

In the operational use:

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

- 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).

BAP mechanism

This security functionality ensures the BAP is correctly performed. It can only be performed once the TOE is personalized with the Triple DES Document Basic Access keys the Personalization Agent loaded beforehand during the personalization phase. Furthermore, this security functionalities ensures the session keys are destroyed at the end of each BAP session.

EAC mechanism

This security functionality ensures the EAC is correctly performed. In particular:

- It handles the certificate verification
- The management of the current date (update and control towards the expiration date of the incoming certificate)
- The signature verification (in the certificate or in the challenge/response mechanism)

It can only be performed once the TOE is personalized with the chip authentication keys & Root CVCA key(s) the Personnalization Agent loaded during the personalization phase. Furthermore, this security functionalities ensures the authentication is performed as described in [R4].

This security functionalities ensures the session keys for secure messaging are destroyed at each successful Chip Authentication step.

The TOE handles an error counter; after several failure in attempting to strongly authenticate the GIS (the error limit is reached). The TOE also implements countermeasures to protect the TOE; it takes more and more time for the TOE to reply to subsequent wrong GIS authentication attempts.

Personalization

This security functionality ensures the TOE, when delivered to the 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 communication between the TOE and the IFD. After a successful BAP authentication, a secure channel is established based on Triple DES or AES algorithm, and after a successful Chip Authentication, a secure channel is established based on Triple DES/AES algorithms.

This security functionality ensures

- No commands were inserted, modified nor deleted within the data flow
- The data exchanged remain confidential

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.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems
T.Forgery	OT.AC_Pers, OE.Personalization, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Exam_MRD, OE.Exam_MRD_AA, OE.Pass_Auth_Sign, OE.Pass_Auth_Verif
T.Counterfeit	OT.CA_Proof, OE.Auth_Key_MRD, OE.Exam_MRD, OT.AA_Proof, OE.Activ_Auth_Verif, OT.Data_Int_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.Unauthorized_Load	OT.Secure_Load_ACode
T.Bad_Activation	OT.Secure_AC_Activation
T.TOE_Identification_Forgery	OT.TOE_Identification

Table 13- Threats and Security Objectives – coverage

OSP	Security Objectives
P.BAC-PP	OE.BAC-PP
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems
P.Manufact	OT.Identification
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization
P.Activ_Auth	OT.AA_Proof

Table 14 - OSPs and Security Objectives – Coverage

Assumptions	OE
A.MRD_Manufact	OE.MRD_Manufact
A.MRD_Delivery	OE.MRD_Delivery
A.Pers_Agent	OE.Personalization
A.Insp_Sys	OE.Exam_MRD, OE.Prot_Logical_MRD
A.Signature_PKI	OE.Exam_MRD, OE.Pass_Auth_Verif, OE.Activ_Auth_Sign
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems
A.Insp_Sys_AA	OE.Exam_MRD_AA, OE.Prot_Logical_MRD_AA

Table 15 - Assumptions and OE – Coverage

The other rationales are available in the complete ST.

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

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

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

[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 P60x144/080 PVA/PVE(Y/B) with IC dedicated software FW5.0

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

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

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

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

I

L

M

O

P

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

S

T

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