ePass V3 td

Taranis

BAC Passport

Public Security Target

Table of contents

List of figures

1 Security Target introduction

1.1 Security Target identification

General identification:

Title:	Taranis Security Target BAC
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL4 + ALC_DVS.2 + ADV_FSP.5 + ADV_INT.2 + ADV_TDS.4 + ALC_CMS.5 + ALC_TAT.2 + ATE_DPT.3
PP(s):	BSI-CC-PP-055
ITSEF:	Serma Technologies
Certification Body:	ANSSI
Evaluation scheme:	FR

TOE technical identification:

Name:	ePass V3 EAC v2 on P5CD081 in BAC configuration with AA
SAAAAR Rom code:	079161
SAAAAR Optional code:	079223

Chips identification:

IC Reference:	P5CD081/P5CC081/P5CD041 V1A
IC EAL:	EAL5 + ALC_DVS.2 + AVA_VAN.5
IC Certificate:	BSI-DSZ-CC-0555-2009
Chip Manufacturer:	NXP Semiconductors

1.2 Overview of the TOE

The current document aims at defining the functions and assurance security requirements which apply to the Taranis smartcard.

It is composed of both an Integrated Circuit (IC) and an embedded software providing secure data management following ePassport specifications (BAC, EAC) this document is therefore a composite Security Target (ST).

In the following, the smartcard will be called “Target Of Evaluation” or TOE.

The TOE is a versatile device that can be easily configured in order to operate in different modes including BAC ePassport and EAC ePassport,. It possesses a dual interface to perform contact and contactless communications to go beyond current ePassport usages.

This device can be proposed as inlay to integrate in secure document booklet but can also be provided in a regular ID1 format.

2 TOE Description

This part of the Security Target describes the TOE as an aid to the understanding of its security requirements. It addresses the product type, the intended usage and the main features of the TOE.

2.1 TOE usages

State or organisation issues TOEs 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 ePassport 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 TOE 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 TOE in context of this security target contains:

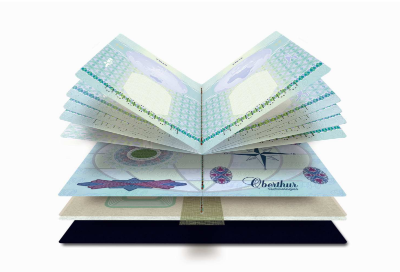
- Visual (eye readable) biographical data and portrait of the holder printed in the booklet
- A separate data summary (MRZ or keydoc data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ or keydoc area)
- And data elements stored on the TOE's chip for contact-less machine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

The authentication of the holder is based on:

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

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

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



The TOE can be viewed as the combination:

- A physical TOE 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 TOE holder
  (1) The biographical data on the biographical data page of the passport book,
  (2) The printed data in the Machine-Readable Zone (MRZ) or keydoc area that identifies the device and
  (3) The printed portrait.
- A logical TOE as data of the TOE holder stored according to the Logical Data Structure as specified by ICAO and extended in [R6], [R7], [R8] on the contactless integrated circuit. It presents contact or contact-less readable data including (but not limited to) personal data of the TOE holder
  (4) The digital Machine Readable Zone Data (digital MRZ data or keydoc data, DG1),

(5) The digitized portraits,
(6) The optional biometric reference data of finger(s) or iris image(s) or both
(7) The other data according to LDS (up to DG24) and
(8) The Document security object.

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

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

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

2.2 TOE architecture

The Target of Evaluation (TOE) is a smartcard composed of the following components:

- An underlying P5CD081, P5CC081 or P5CD041 chip of NXP,
- A native "BIOS FAT" allowing efficient access to chip functionalities,
- A dedicated highly secure cryptographic library,
- A personalisation application on top of the BIOS,
- An LDS application providing both the BAC/EAC features on top of the BIOS.

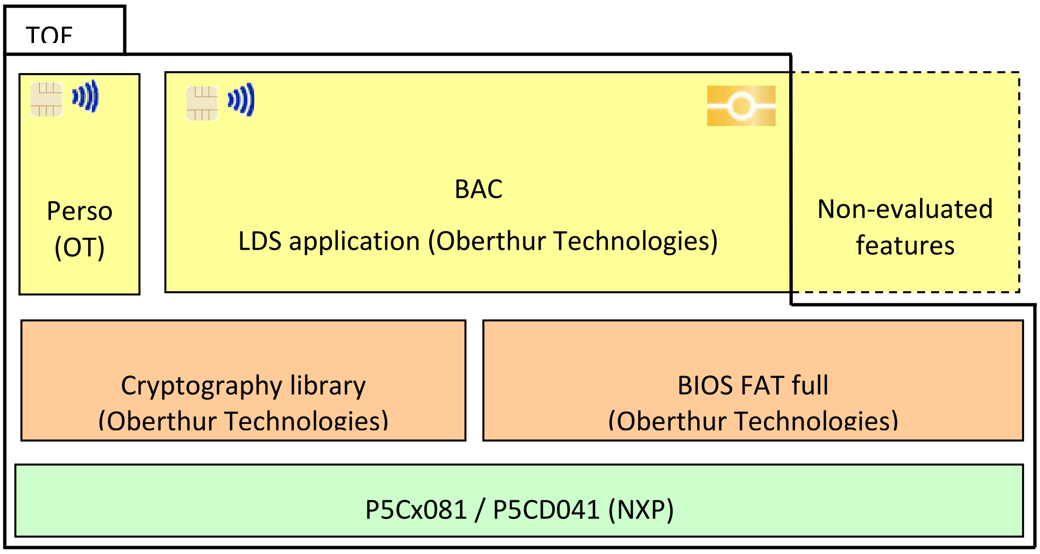


Figure 1 TOE architecture

2.2.1 Integrated Circuit (IC)

The TOE relies on the functional and security features of the P5CD081. This chip is designed to embed the secure code of Oberthur Technologies for the production of smart cards.

This chip provides the following major features:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- A FameXE Enhanced Pulbic key coprocessor especially for RSA and ECC,
- A 3DES coprocessor,
- An AES coprocessor,
- AIS-31 class P2 compliant Random Number Generator,
- A CRC calculation block.

For more details, see [R14].

2.2.2 Basic Input/Output System (BIOS)

The native BIOS of 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.

2.2.3 Cryptographic library

A dedicated cryptographic library is is designed and embedded on the TOE to provide the highest security level and best tuned performances. It provides the following algorithms:

Feature	Embedded
SHA-1, SHA-224, SHA 256, SHA-384 and SHA-512 bits	✔
RSA CRT from 1024, to2048 bits (by steps of 256 bits)	✔
RSA SFM from 1024 to 2048 bits (by steps of 256 bits)	✔
ECC with key sizes from 192 to 521bits	✔
3DES with 112 bits key size	✔
AES with 128, 192, 256 key sizes	✔

2.2.4 Resident application

This application manages the TOE in pre-personalisation, personalisation and use phase in order to configure the card in the expected way.
It implements and control access to the following services:

- MSK management,
- File management including data reading and writing,
- Key generation,
- Key injection,
- PIN management,
- Locks management.

The resident application can be addressed:

- in clear mode for secure environment or non-sensitive commands,
- using a 3DES secure channel otherwise.

2.2.5 LDS application

The Logical Data Structure (LDS) application is a generic filesystem that can be configured to match especially ICAO specifications for ePassports BAC and EAC.
ISO specifications for IDL BAP and EAP are also matched, but not in the TOE scope.
It also includes commands and protocol management specified in [R15] used to grant access to sensitive data stored in the filesystem.

Here are the main features provided by the LDS application and present in the evaluation scope:

Feature	Embedded	In the ST scope[1]	References
BAC	✓	✓	[R2], [R3]
EAC	✓	✗	[R2], [R3], [R4]
Active Authentication (RSA CRT/SFM and ECC)	✓	✓	[R2], [R3]
Cryptosystem migration (Algorithm change during certificate verification transaction)	✓	✗	[R2], [R3], [R4]
BAP	✓	✗	[R6], [R7], [R8]
EAP	✓	✗	[R6], [R7], [R8]

2.2.5.1 Basic Access Control (BAC)

The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system

- reads the printed data in the MRZ (for ePassport),

[1] Features not included in the present Security Target are covered in the context of other CC certificates of the same product.

- authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

2.2.5.2 Basic Access Protection (BAP)

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.

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.

This feature is not in the TOE scope.

2.2.5.3 Active Authentication (AA)

The Active Authentication of the TOE is an optional feature that may be implemented. It ensures that the TOE has not been substituted, by means of a challenge-response protocol between the inspection system and the TOE. For this purpose the chip contains its own Active Authentication RSA or ECC Key pair. A hash representation of Data Group 15 (DG15, see 2.5.1) Public Key is stored in the Document Security Object (SOD, see 2.5.1) 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.

2.2.5.4 Extended Access Control (EAC)

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

2.2.5.5 Extended Access Protection (EAP)

The Extended Access Protection (EAP) extends EAC to allow a more flexible protocol. It can protect up to 16 DGs (from 1 to 16) and is no more restricted to DG3 and 4. There is also no prerequisite to perform A BAP before starting EAP. In addition, it is possible to send more than 2 certificates to the TOE in order to gain extra access rights.

Following secure messaging can be either in 3DES or AES taking into account that if a BAP was previously performed algorithm used must be stronger[2].

This feature is not in the TOE scope.

2.3 Chip and software composition

The TOE contains an auto-programmable microcomputer (IC) with non-volatile EEPROM memory, permitting the storing of secret or confidential data, and with associated circuits that ensure its protection. The IC also integrates a ROM memory which embeds the code software of the smartcard.

In order to ensure a secure composition between IC and software, the chip is configured and used according to the security requirements specified in the datasheet and associated guides. This especially specifies the secure way to manage IC memory.

The optional code or "codop" is an executable code that is stored in the EEPROM of the chip. This code is called by the Resident Application when needed. These data are loaded during the pre-personalisation phase after the authentication of the manufacturer. Once an optional code is loaded, it is not possible to load any other optional code whether the TOE is in pre-personalisation phase or personalisation phase. The TOE ensures the optional code's integrity and that it can not be read from the outside.

In order to configure the available features of the product a One-Time Programmable (OTP) area is present (see 2.4). It can be written only once and cannot be erased afterward.

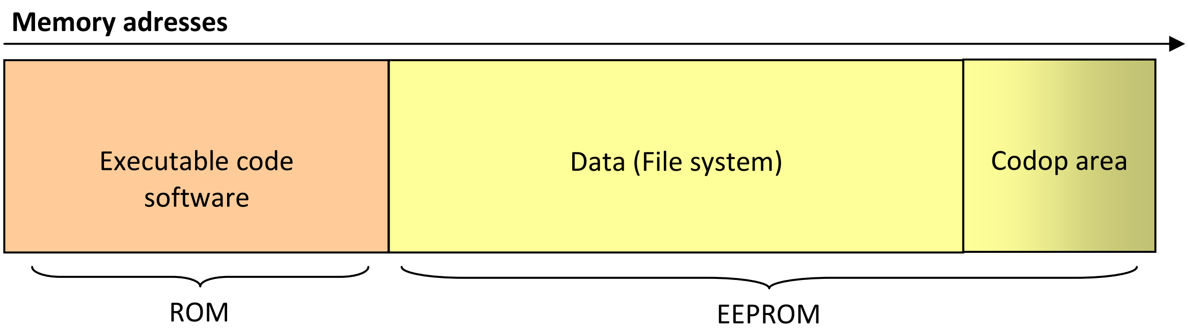


Figure 2 Memory mapping of the TOE

2.4 TOE Configurations

The application locks are within a particular area of the EEPROM memory. It is called OTP (One Time Programmable). When the TOE is delivered, all the bits of this area are set to '0'. Theses bits may be set (to "1") in pre-personalisation phase or personalisation phase after the agent authentication (Manufacturer or Personnalizer). Once a bit is set to "1" in this area, it can not be reset anymore. This area is used to select the configuration of the TOE, in particular:

- If the BAC is enforced in used phase ('0' = not enforced/'1' = enforced)
- If the EAC is enforced in used phase ('0' = not enforced/'1' = enforced)
- If the Get Data command is disabled ('0' = enabled/'1' = disabled)
- If the Active authentication is activated ('0' = not activated/'1' = activated)

[2] AES 256 is stronger than AES 192 which is stronger than AES 128 which is stronger than 3DES.

- To indicate the TOE was pre-personalised ('1' = pre-personalised)
- To indicate the TOE was personalised ('1' = personalized)

These OTP bytes are protected in integrity as they are copied in EEPROM too.

Final configuration of the product is set by activating one or several of the five first locks. The product is in use phase when the two last locks are activated. Since BAC is a configuration, the two ones have been merged into a unique lock.

Note that in order to be functional, a correct and consistent personalisation of the TOE must be performed.

2.5 TOE logical structure

Roughly, the embedded application, when powered, is seen as a master file, containing a Dedicated file (DF) for the LDS.
This dedicated file is selected by means of the Application Identifier (AID) of the LDS application for example in case of ePassport. Once the application dedicated files are selected, the file structure it contains may be accessed, provided the access conditions are fulfilled.

2.5.1 File structure of the TOE

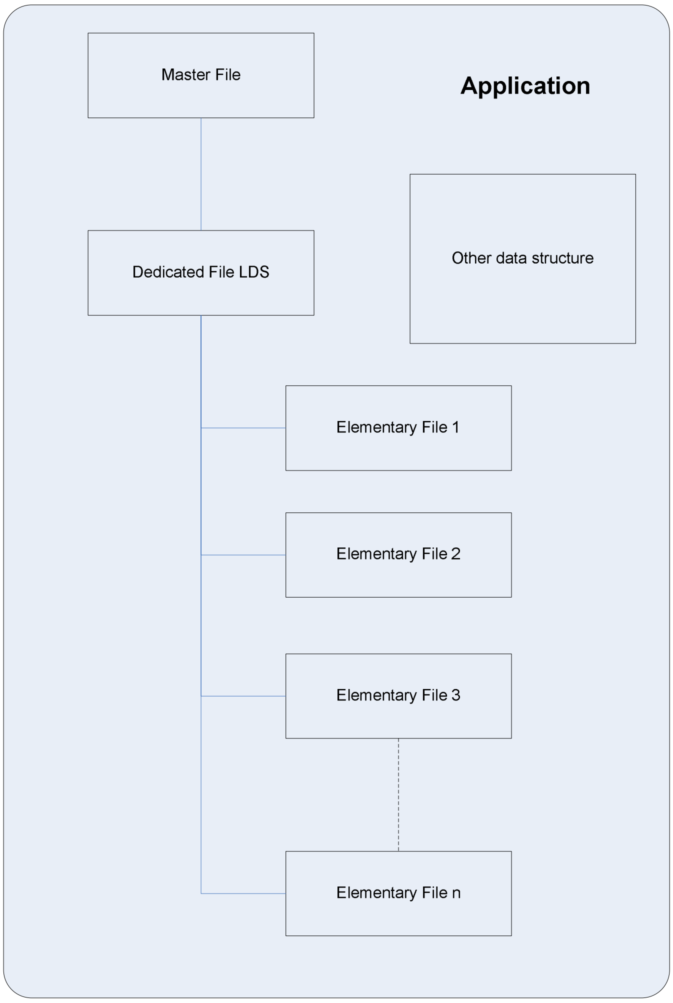


Figure 3 : Structure of the file system

The TOE distinguish between two types of data

- System files,
- Data files that store data that are visible from the outside.

Basically, system files and data files are files handled by the Resident Application. The Resident Application handles their creation and management. Both types have the following characteristics:

- Size, size reserved within the EEPROM for the content of this file,
- EF ID, Elementary File Identifier of the file within the file structure,
- SFI, Short File Identifier used for an easy file selection. It is only used for data files,
- Access conditions, it specify under which conditions the file may be accessed (read never, read always...).

2.5.2 System files

System files are dedicated to store sensitive data that are used by the application. These data are protected in integrity by means of a checksum. Theses files may be created and updated in pre-personalisation or personalisation phase. Files containing keys are never readable.
Once created, these files are used by the application to work properly. They have to be created before any use of the application.

In particular, theses files are used to store:

- The active authentication public key needed to perform the active authentication,
- The active authentication private key needed to perform the active authentication,
- The keys needed to perform BAC and EAC,
- The list of the application present on the card.

2.5.3 Data files

Data files also called Elementary files (EF) or Data Groups (DG) are dedicated to store data that may be retrieved. They are protected in integrity by means of a checksum and can be created or updated either in pre-personalisation or in personalisation phase. They are also created in such a way they can only be read or write in use phase, provided authentications specified in access rights are performed.

All personalisation configurations are possible including BAC and EAC. Nevertheless, Data Files usually considered are the following:

- EF.COM which describes which DGs are present in the file structure,
- EF.SOD which contains a certificate computed over the whole DGs. It ensures their integrity & authenticity,
- DG1 up to DG24 which contains information about the holder (picture, name…) and key required to perform authentications.

2.6 Non evaluated features

Some features of the product are put out of the evaluation scope and are therefore not part of the TOE. Here is the complete list of those functionalities:

- Supplemental Access Control,
- Standard and biometric PIN management (therefore PIN associated commands are out of scope),
- BAP and EAP applications

2.7 TOE life cycle

The Smart card life-cycle considered hereby, is the one described in [R13]. This protection profile is decomposed into 7 phases, described hereafter, whose only first three ones defined the TOE evaluation scope.

This life cycle is related to the different phases the designer/manufacturer/issuer has to go through to get a smart card ready to use. It starts from the design till the end of usage of the card.

Note that [R10] and [R11] define an alternative lifecycle almost equivalent (phases in [R13] are steps in [R10] and [R11]) except this only difference:

- Step 4 in [R10] and [R11], correspond to phase 4 of [R10] and [R11] and blocks ‘Micromodule”, “testing” and “Embedding” in phase 5 of [R10] and [R11],
- Step 5 in [R10] and [R11] correspond to the only next blocks “Personnalisation” and “Testing” in phase 5 of [R10] and [R11].

It is depicted in the figure below:

Personalisation and Pre-personnalisation

TOE usage

TOE scope

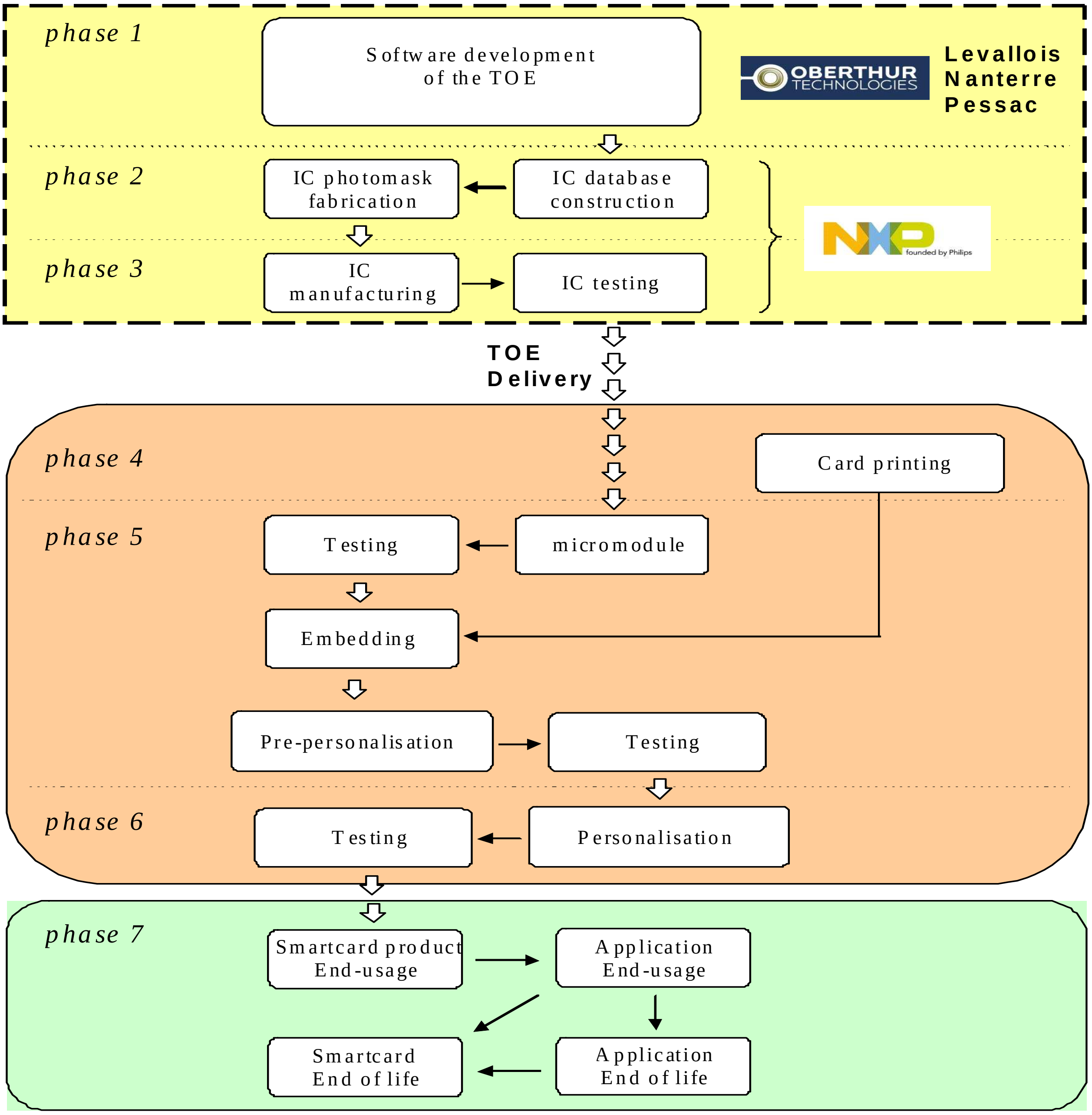


Figure 4 Smartcard product life-cycle for the TOE

3 Conformance claims

3.1 Common Criteria conformance

This Security Target (ST) is CC Part 2 extended [R35] and CC Part 3 conformant [R36] and written according to the Common Criteria version 3.1 Part 1 [R34].

3.2 Package conformance

This ST is conformant to the EAL4 package as defined in [R36].

The EAL4 have been augmented[3] with the following requirements to fulfill the Oberthur Technologies assurance level:

Requirement	Name	Type
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
ADV_FSP.5	Complete semi-formal functional specification with additional error information	Higher hierarchical component
ADV_INT.2	Well-structured internals	New component
ADV_TDS.4	Semiformal modular design	Higher hierarchical component
ALC_CMS.5	Development tools CM coverage	Higher hierarchical component
ALC_TAT.2	Compliance with implementation standards	Higher hierarchical component
ATE_DPT.3	Testing: modular design	Higher hierarchical component

Remark

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

3.3 Protection Profile conformance

The Security Target claims strict conformance to the following PP written in CC3.1 revision 3:

- Machine Readable Travel Documents with “ICAO Application”, Basic Access Control [R10].

[3] This EAL and its augmentations correspond to an EAL5+ALC_DVS.2 where AVA_VAN level is downgraded to AVA_VAN.3 following constraint of [R10] about MRZ/keydoc entropy.

4 Security problem definition

4.1 Assets

Logical MRTD data

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

The Active Authentication Public Key Info in DG 15 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 MRTD.

All these data may be sorted out in two different categories.

- If they are specific to the user, they are User data,
- If they ensures the correct behaviour of the application, they are TSF Data.

User data

CPLC Data	Data uniquely identifying the chip. They are considered as user data as they enable to track the holder
Personnal Data of the MRTD holder (EF.DGx, except EF.DG15)	Contains identification data of the holder
Document Security Object (SOD) in EF.SOD	Contain a certicate ensuring the integrity of the file stored within the MRTD and their authenticity. It ensures the data are issued by a genuine country
Common data in EF.COM	Declare the data the travel document contains
Active Authentication Public Key in EF.DG15	Contain public data enabling to authenticate the chip thanks to an active authentication

TSF data

TOE_ID	Data enabling to identify the TOE
Personalisation Agent reference authentication Data	Private key enabling to authenticate the Personalisation agent
Basic Access Control (AC) Key	Master keys used to established a trusted channel between the Basic Inspection Terminal and the travel document
Active Authentication private key	Private key the chip uses to perform an active authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity
Life Cycle State	Life Cycle state of the TOE

Authenticity of the MRTD's chip

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

4.2 Threats

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

T.Chip_ID

Adverse action: An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD"s chip by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance

Asset: Anonymity of user

T.Skimming

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: confidentiality of logical MRTD data.

T.Eavesdropping

Adverse action: An attacker is listening to an existing communication between the MRTD"s chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.

Asset: confidentiality of logical MRTD data.

T.Forgery

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

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

Asset: authenticity of logical MRTD data.

T.Abuse-Func

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

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

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

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

T.Information_Leakage

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

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

Asset: confidentiality of logical MRTD and TSF data.

T.Phys-Tamper

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

MRTD"s chip, (ii) modify security functions of the MRTD"s chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.

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

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

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

T.Malfunction

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD"s chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD"s chip Embedded Software.

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

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

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

T.Counterfeit

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

4.3 Organisational Security Policies

P.Manufact

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

P.Personalization

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

P.Personal_Data

The biographical data and their summary printed in the MRZ and stored on the MRTD"s chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)3 and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD"s chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD"s chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [R2].

P.Sensitive_Data_Protection

All the sensitive data are at least protected in integrity. The keys are protected in both integrity and confidentiality.

P.Key_Function

All the cryptographic routines are designed in such a way that they are protected against probing and do not cause any information leakage that may be used by an attacker.

4.4 Assumptions

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

A.MRTD_Manufact

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

A.MRTD_Delivery

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

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

A.Pers_Agent

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

A.Insp_Sys

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [R2]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

A.BAC-Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [R2], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

5 Security Objectives

5.1 Security Objectives for the TOE

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

OT.AC_Pers

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R2] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

OT.Data_Int

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT.Data_Conf

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

OT.Identification

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

OT.Prot_Abuse-Func

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

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

OT.Prot_Inf_Leak

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

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

OT.Prot_Phys-Tamper

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

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

with a prior

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

OT.Prot_Malfunction

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

OT.Chip_Authenticity

The TOE must support the Inspection Systems to verify the authenticity of the MRTD's chip. The TOE stores a RSA or ECC private key to prove its identity, and that is used in chip authentication. This mechanism is described as "Active Authentication".

5.2 Security objectives for the Operational Environment

5.2.1 Issuing State or Organization

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

OE.MRTD_Manufact

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

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

OE.MRTD_ Delivery

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

- o non-disclosure of any security relevant information,
- o identification of the element under delivery,
- o meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- o physical protection to prevent external damage,
- o secure storage and handling procedures (including rejected TOE"s),
- o 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 State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [R2].

OE.BAC-Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [R2] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

5.2.2 Receiving State or Organization

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

OE.Exam_MRTD

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [R2].

OE.Passive_Auth_Verif

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

OE.Prot_Logical_MRTD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD 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).

6 Extended requirements

6.1 Extended families

6.1.1 Extended family FAU_SAS - Audit data storage

6.1.1.1 Description

see [PP-0055].

6.1.1.2 Extended components

6.1.1.2.1 Extended component FAU_SAS.1

Description

see [PP-0055].

Definition

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 [PP-0055].

6.1.1.3 Rationale

see [PP-0055].

6.1.2 Extended family FCS_RND - Generation of random numbers

6.1.2.1 Description

see [PP-0055].

6.1.2.2 Extended components

6.1.2.2.1 Extended component FCS_RND.1

Description

See [PP-0055].

Definition

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 [PP-0055].

6.1.2.3 Rationale

see [PP-0055].

6.1.3 Extended family FMT_LIM - Limited capabilities and availability

6.1.3.1 Description

See [PP-0055].

6.1.3.2 Extended components

6.1.3.2.1 Extended component FMT_LIM.1

Description

See [PP-0055].

Definition

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 [PP-0055].

6.1.3.2.2 Extended component FMT_LIM.2

Description

See [PP-0055].

Definition

FMT_LIM.2 Limited availability

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

Dependencies: (FMT_LIM.1)

Rationale

See [PP-0055].

6.1.3.3 Rationale

See [PP-0055].

6.1.4 Extended family FPT_EMS - TOE Emanation

6.1.4.1 Description

See [PP-0055].

6.1.4.2 Extended components

6.1.4.2.1 Extended component FPT_EMS.1

Description

See [PP-0055].

Definition

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 [PP-0055].

6.1.4.3 Rationale

See [PP-0055].

7 Security Functional Requirements

7.1 Security Functional Requirements

7.1.1 PP BAC

FAU_SAS.1 Audit storage

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

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Key Derivation Algorithm** and specified cryptographic key sizes **112 bits** that meet the following: **[R2], normative appendix 5**.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

FCS_COP.1/ENC Cryptographic operation

FCS_COP.1.1/ENC The TSF shall perform **secure messaging (BAC) - encryption and decryption**

in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3 [R27] normative appendix 5, A5.3**.

FCS_COP.1/AUTH Cryptographic operation

FCS_COP.1.1/AUTH The TSF shall perform **symmetric authentication, encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112** that meet the following: **FIPS 46-3 [R27]**.

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging - message authentication code**

in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bits** that meet the following: **ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)**.

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **the requirement to provide an entropy of at least 7.976 bits in each byte, following AIS 31 [R31]**.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within range of acceptable values 0 to 255 consecutive** unsuccessful authentication attempts occur related to **BAC authentication protocol**.

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **1. to read the Initialization Data in Phase 2 "Manufacturing",**
- **2. to read the random identifier in Phase 3 "Personalization of the MRTD",**
- **3. to read the random identifier in Phase 4 "Operational Use"**

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

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **1. to read the Initialization Data in Phase 2 "Manufacturing",**
- **2. to read the random identifier in Phase 3 "Personalization of the MRTD",**
- **3. to read the random identifier in Phase 4 "Operational Use"**

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

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

FIA_UAU.4 Single-use authentication mechanisms

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

- **1. Basic Access Control Authentication Mechanism,**
- **2. Authentication Mechanisms based on Triple-DES and AES**.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

- **1. Basic Access Control Authentication Mechanism**
- **2. Symmetric Authentication Mechanism based on Triple-DES and AES**

to support user authentication.

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

- **1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s):**
  - **the Symmetric Authentication Mechanism with the Personalization Agent Key,**
- **2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys**.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism**.

FDP_ACC.1 Subset access control

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

FDP_ACF.1 Security attribute based access control

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

- **1. Subjects:**
  - **a. Personalization Agent,**
  - **b. Basic Inspection System,**
  - **c. Terminal,**
- **2. Objects:**
  - **a. data EF.DG1 to EF.DG16 of the logical MRTD,**
  - **b. data in EF.COM,**
  - **c. data in EF.SOD,**
  - **d. Active Authentication public key,**
- **3. Security attributes**
  - **a. authentication status of terminals**.

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

- **1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, including the Active Authenticate public Key,**
- **2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, including the Active Authenticate public Key**.

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

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

- **1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4**.

FDP_UCT.1 Basic data exchange confidentiality

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

FDP_UIT.1 Data exchange integrity

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

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

FMT_SMF.1 Specification of Management Functions

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

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

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **1. Manufacturer,**
- **2. Personalization Agent,**
- **3. Basic Inspection System**.

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

FMT_LIM.1 Limited capabilities

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

Deploying Test Features after TOE Delivery does not allow

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

FMT_LIM.2 Limited availability

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

Deploying Test Features after TOE Delivery does not allow

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

FMT_MTD.1/INI_ENA Management of TSF data

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

FMT_MTD.1/INI_DIS Management of TSF data

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

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys and Active Authentication private key** to **Personalization Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the **Document Basic Access Keys, Personalisation Agent keys and Active Authentication private key** to **none**.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Keys** and **Active Authentication private key**.

FPT_EMS.1.2 The TSF shall ensure **any unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Keys** and **Active Authentication private key**.

FPT_FLS.1 Failure with preservation of secure state

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

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

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions**

- **At reset**
- **Before the first execution of the optional code,**
- **After the Active Authentication is computed,**
- **Before any cryptographic operation,**
- **When accessing a DG,**
- **Prior to any use of TSF data,**
- **Before execution of any command,**
- **When performing a BAC authentication,**

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

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

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

FPT_PHP.3 Resistance to physical attack

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

7.1.2 Active Authentication (AA)

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.

FCS_COP.1/SIG_MRTD Cryptographic operation

FCS_COP.1.1/SIG_MRTD The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **RSA CRT, RSA SFM or ECDSA with SHA1, SHA-224, SHA-256, SHA-384 or SHA-512** and cryptographic key sizes

- **1024 to 2048 bits for RSA (by steps of 256bits),**
- **192 to 521 bits for ECDSA,**

that meet the following:

- **scheme 1 of [R20] for RSA,**
- **[R17], [R18], [R19] for ECC**.

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

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

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

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

FMT_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**.

FCS_CKM.1/ASYM Cryptographic key generation

FCS_CKM.1.1/ASYM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA & ECC** and specified cryptographic key sizes

- **1024 to 2048 bits for RSA (by steps of 256 bits),**
- **192 to 521 bits over characteristic p curves for ECC**

that meet the following: **[R20], [R21], [R22], [R23]**.

7.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3.

8 TOE Summary Specification

8.1 TOE Summary Specification

Access Control in reading

This function controls access to read functions (in EEPROM) 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:

- BAC keys
- Active Authentication private key
- Personalisation agent 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, the Document Security Object, EF.COM only after BAC authentication and through a valid secure channel.

In the personalisation phase

- The personalisation 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 EEPROM can be accessed at anytime

Access Control in writing

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

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

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

In the personalisation phase

- The personalisation 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.

BAC mechanism

This security functionality ensures the BAC is correctly performed. It can only be performed once the TOE is personalized with the symmetric BAC keys the Personalization Agent loaded beforehand during the personalization phase. Furthermore, this security functionalities ensures the session keys are destroyed at the beginning of each BAC session. A self-test on TDES and random generator is performed when a BAC session is requested.

Secure Messaging

This security functionality ensures the confidentiality & integrity of the channel the TOE and the IFD are using to communicate. After a successful BAC authentication, a secure channel is established based on Triple DES algorithms. This security functionality ensures

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

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

Personalisation Agent Authentication

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.

Active Authentication

This security functionality ensures the Active Authentication is performed as described in [R2]. (if it is activated by the personnalizer). A self-test on the random generator is performed priori to any Active authentication. Moreover, this security functionality is protected against the DFA.

Self tests

The TOE performs self tests on the TSF data it stores to protect the TOE. In particular, it is in charge of the:

- DFA detection for the Active authentication
- Self tests of the random generator before the BAC and Active Authentication
- Self tests of the DES before the BAC Monitoring of the integrity of keys, files and TSF data Monitoring the integrity of the optional code (at start up) Protecting the cryptographic operation

The integrity of the files are monitored each time they are accessed and the integrity of the optional code is checked each time the TOE is powered on. The integrity of keys and sensitive data is checked each time they are used/accessed.

Safe state management

This security functionalities ensures that the TOE gets bask 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.

Physical protection

This security functionality protects the TOE against physical attacks.

Prepersonalisation

This function is in charge of pre-initializing the product and loading patch code if needed.

8.2 Link between the SFR and the TSF

	Access Control in reading	Access Control in writing	BAC mechanism	Secure Messaging	PA Authentication	Active Authentication	Self tests	Safe state management	Physical protection	Prepersonalisation
FAU_SAS.1								X	X	
FCS_CKM.1				X						
FCS_CKM.4			X	X						
FCS_COP.1/SHA			X		X	X				X
FCS_COP.1/ENC			X	X		X				X
FCS_COP.1/AUTH			X			X				X
FCS_COP.1/MAC			X	X						X
FCS_RND.1			X	X	X	X	X			X
FIA_AFL.1			X							
FIA_UID.1	X		X	X						X
FIA_UAU.1	X		X	X						
FIA_UAU.4	X		X	X						
FIA_UAU.5	X		X	X						
FIA_UAU.6	X		X	X						
FDP_ACC.1	X	X				X				
FDP_ACF.1	X		X			X				
FDP_UCT.1	X		X							
FDP_UIT.1	X		X							
FMT_SMF.1		X			X			X		X
FMT_SMR.1								X		
FMT_LIM.1								X	X	
FMT_LIM.2								X	X	

	Access Control in reading	Access Control in writing	BAC mechanism	Secure Messaging	PA Authentication	Active Authentication	Self tests	Safe state management	Physical protection	Prepersonalisation
FMT_MTD.1/INI_ENA		X			X					X
FMT_MTD.1/INI_DIS	X									
FMT_MTD.1/KEY_WRITE		X				X				
FMT_MTD.1/KEY_READ	X					X				
FPT_EMS.1			X		X	X				X
FPT_FLS.1*								X		
FPT_TST.1							X			
FPT_PHP.3									X	
FDP_DAU.1/AA						X				
FCS_COP.1/SIG_MRTD			X			X				
FDP_ITC.1/AA		X				X				
FMT_MOF.1/AA						X				
FCS_CKM.1/ASYM						X				

9 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] 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

[R4] Advanced Security Mechanisms for Machine readable travel documents – Extended Access control (EAC) – TR03110 – v1.11

[R5] 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

[R6] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 1:Physical characteristics and basic data set, ISO/IEC FDIS 18013-1:2005(E)

[R7] Information Technology - Personal Identification — ISO Compliant Driving Licence — Part 2: Machine-readable technologies, ISO/IEC FDIS 18013-2:2007(E)

[R8] Personal Identification — ISO Compliant Driving Licence — Part 3: Access control, authentication and integrity validation, ISO/IEC FDIS 18013-3:2008(E)

Protection Profiles

[R9] Smartcard IC Platform Protection Profile v 1.0 - BSI-PP-0035 15/06/2007

[R10] Machine readable travel documents with “ICAO Application”, Basic Access control – BSI-PP-0055 v1.10 25th march 2009

[R11] Machine readable travel documents with “ICAO Application”, Extended Access control – BSI-PP-0056 v1.10 25th march 2009

[R12] E-passport: adaptation and interpretation of e-passport Protection Profiles, SGDN/DCSSI/SDR, ref. 10.0.1, February 2007

[R13] Embedded Software for Smart Security Devices, Basic and Extended Configurations, ANSSi-CC-PP-2009/02, 1/12/2009

Security Target

[R14] NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cc081VIA Security Target Lite, BSI-DSZ-0555, Rev. 1.3, 21 September 2009

Standards

[R15] ISO7816-4 – Organization, security and commands for interchange

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Misc

[R31] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[R32] NOTE-10 - Interpretation with e-passport PP_courtesy translation-draft v0.1

CC

[R33] 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

[R34] Common Criteria for Information Technology security Evaluation Part 2 : Security Functional Components, CCMB-2012-09-002, version 3.1 Revision 4 Final, September 2012

[R35] Common Criteria for Information Technology security Evaluation Part 3 : Security Assurance Components, CCMB-2012-09-003, version 3.1 Revision 4 Final, September 2012

10 ACRONYMS

AA	Active Authentication
BAC	Basic Access Control
CC	Common Criteria Version 3.1 revision 3
CPLC	Card personalisation 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
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
SFI	Short File identifier
SHA	Secure hashing Algorithm
SOD	Security object Data
TOE	Target of Evaluation
TSF	TOE Security function

Index