Oberthur Technologies

ID One ePass V2.2 on NXP in EAP configuration with AA

Public Security Target

Table of contents

List of figures

List of tables

1 Security Target introduction

1.1 Security Target identification

General identification:

Title:	ePass v2.2 on NXP Security Target EAP with AA
Editor:	Oberthur Technologies
CC version:	3.1 revision 3
EAL:	EAL5 + ALC_DVS.2 + AVA_VAN.5
PP(s):	BSI-CC-PP-056

TOE technical identification:

Name:	ePass v2.2 on NXP P5CD081 in EAP configuration with AA
SAAAAR Rom code:	075021
SAAAAR Optional code:	076151

Chips identification:

IC Reference:	P5CD081 V1A of NXP
IC EAL:	EAL5 + ALC_DVS.2 + AVA_VAN.5
IC Certificate:	BSI-DSZ-CC-0555-2009

1.2 Overview of the TOE

The current document aims at defining the functions and assurance security requirements which apply to the ePass v2.2 on NXP smartcard.

It is composed of both an Integrated Circuit (IC) and an embedded software providing secure data management following ePassport specifications (BAC, EAC) and driving licence specifications (BAP, EAP); 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, EAC ePassport, BAP driving licence and EAP driving licence. 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 credit card format especially in driving licence configurations.

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.

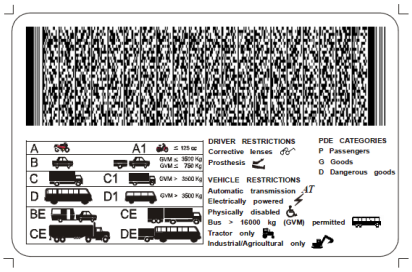
2.1 TOE usages

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 or checking driving licence validity during a police control.

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 "driving licence penalty points", "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 MRD'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 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 and BAP/EAP features on top of the BIOS.

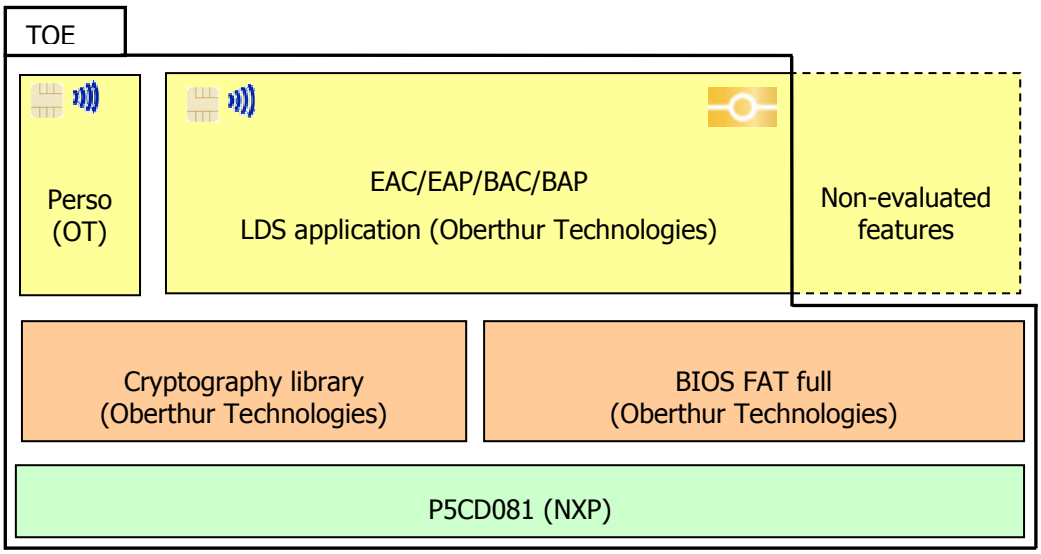


Figure 1 TOE architecture[1]

[1] OT is the acronym of Oberthur Technologies.

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 and ISO specifications for IDL BAP and EAP.
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[2]	References
BAC	✔	✔	[R1],[R2], [R3], [R5]
EAC	✔	✘	R1],[R2], [R3], [R4], [R5]
Active Authentication (RSA CRT/SFM and ECC)	✔	✔	[R1],[R2], [R3], [R5]
Cryptosystem migration (Algorithm change during certificate verification transaction)	✔	✘	R1],[R2], [R3], [R4], [R5]
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),
- 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] Features not included in the present Security Target are covered in the context of other CC certificates of the same product.

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.

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[3].

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.

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

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.

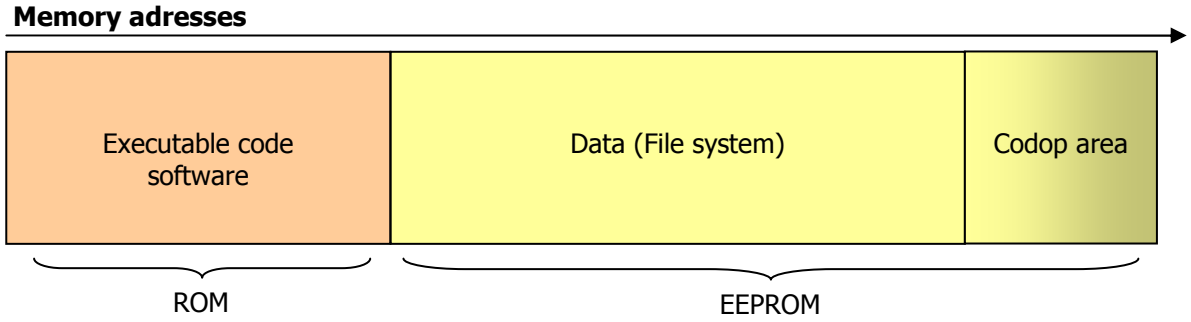


Figure 2 Memory mapping of the TOE

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/BAP 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 EAP 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)
- 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 BAP configuration, the two ones have been merged into a unique lock. Nevertheless, usage of AES keys identifies BAP configuration.

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

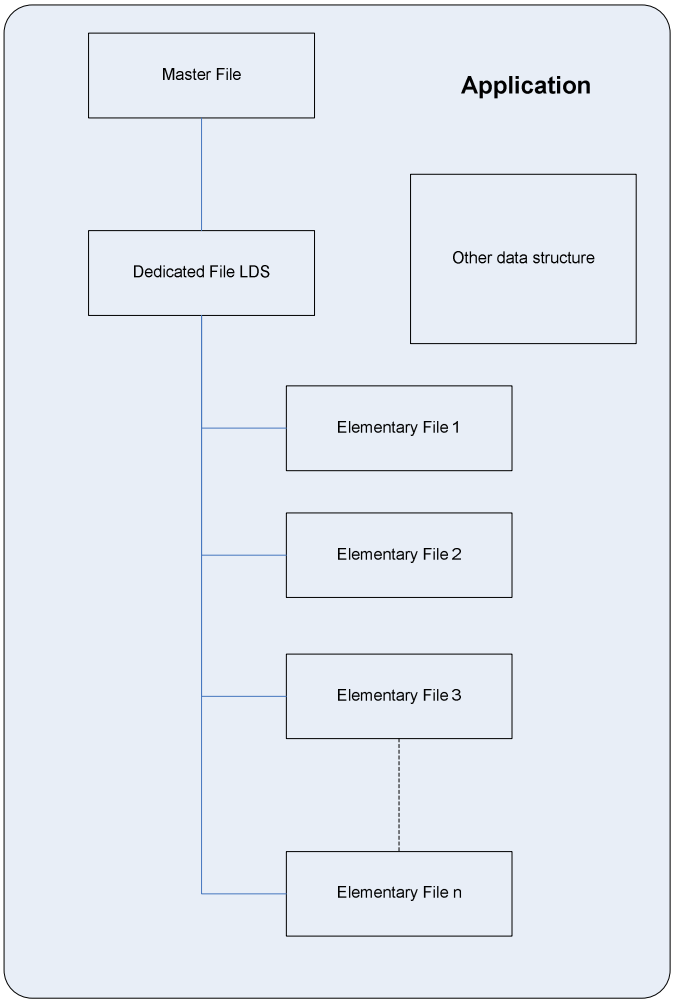


Figure 3 : Structure of the file system

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, BAP, EAC and EAP,
- 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),

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 anternative 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:

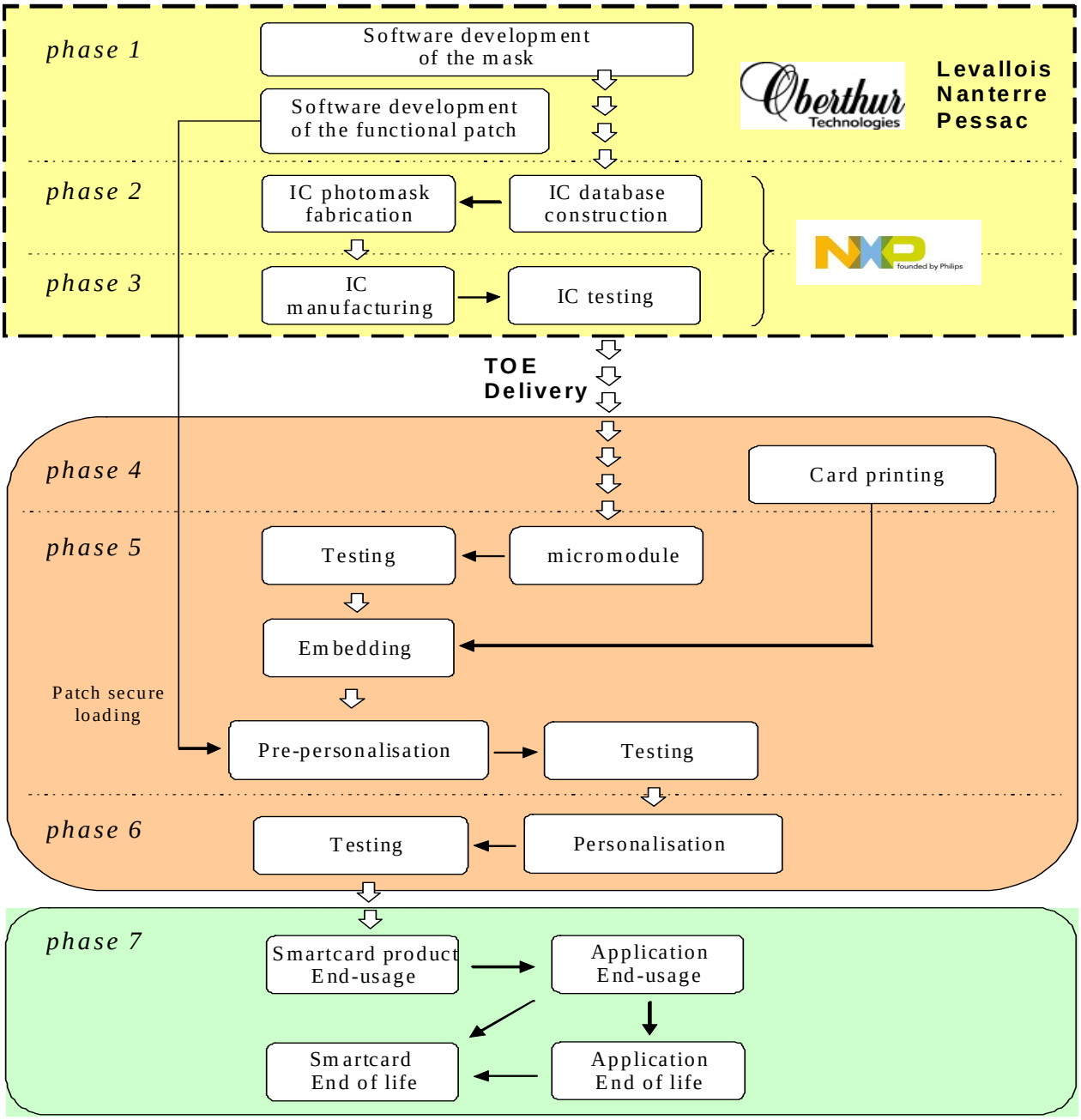


Figure 4 *Smartcard product life-cycle for the TOE*

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 EAL5 package as defined in [R36].

The EAL5 have been augmented with the following requirements to fulfill the Oberthur Technologies assurance level**:**

Requirement	Name	Type
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VAN.5	Advanced methodical vulnerability analysis	Higher hierarchical component

3.3 Protection Profile conformance

The Security Target is based on the following PP written in CC3.1 revision 3:

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

4 Security problem definition

4.1 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], [R6], [R7] and [R8]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. Depending on the personalisation, the EF.DG1 to EF.DG24 can contain personal data of the MRD holder. The Chip Authentication Public Key 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 EAP Security Target is dedicated to the protection of both Active Authentication (see below) and highly sensitive data. The other one (and associated keys) are described and managed in the related BAP Security Target.

The Active Authentication Public Key Info 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 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
Highly sensitiv reference data	Contain especially the fingerprint and the iris picture
Chip Authentication Public Key	Contain public data enabling to authenticate the chip thanks to a chip authentication
Active Authentication Public Key	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 (same as BAP ST)
Basic Access Protocol Keys	Master keys used to established a trusted channel between the Basic Inspection Terminal and the MRD (same as BAP ST)
Chip Authentication private Key	Private key the chip uses to perform a chip authentication
Active Authentication private key	Private key the chip uses to perform an active authentication
Session keys for the secure channel	Session keys used to protect the communication in confidentiality and in integrity
Life Cycle organisation	Life Cycle organisation of the TOE
Public Key True Root Certificate	Trust point of the travel document stored in persistent memory
True Root Certificate Certificate	All the data related to the True Root Certificate key (expiration date, name,..) stored in persistent memory
Current Date	Current date of the travel document

Authenticity of the MRD's chip

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

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.Read_Sensitive_Data

Adverse action: An attacker tries to gain the highly sensitive 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 (highly sensitive 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 highly sensitive 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. highly sensitive reference) data

T.Forgery

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 highly sensitive 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 passport book, in the printed keydoc and in the digital keydoc to claim another identity of the holder. 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 highly sensitive 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 highly sensitive reference finger data read from the logical MRD of a holder 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 ehigh 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 "Operational Use" phase 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 organisation after delivery to MRD holder.

Threat agent: having high 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 high 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 highly sensitive reference data for the inspection system) or TSF Data (e.g. authentication key of the MRD'' 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 high 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 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 high attack potential, being in possession of a legitimate MRD.

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

4.3 Organisational Security Policies

P.BAP-PP

The issuing organisations or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRD data DG1, DG2, DG5 to DG24 if specified in EF.SOD as well as to the data groups Common and Security Data. The MRD is successfully evaluated and certified, based on the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [R10] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRD data.

P.Sensitive_Data

The highly sensitive reference data are sensitive private personal data of the MRD holder. The highly sensitive 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 organisation authorizes the Document Verifiers of the receiving organisations 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 organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the highly sensitive 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 organisation only.

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.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 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 organisation (i) examining an MRD presented by the holder and verifying its authenticity and (ii) verifying the holder as MRD holder. The Basic Inspection System for global interoperability (i) includes the Organisation Signing CA Public Key and the Document Signer Public Key of each issuing organisation, and (ii) implements the terminal part of the Basic Access Protocol [R8]. The Basic Inspection System reads the logical MRD under Basic Access Protocol 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 organisation through the Document Verifier of the receiving organisation to read the highly sensitive reference data.

A.Signature_PKI

The issuing and receiving organisations or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRD. The issuing organisation runs a Certification Authority (CA) which securely generates, stores and uses the Organisation Signing CA Key pair. The CA keeps the Organisation Signing CA Private Key secret and is recommended to distribute the Organisation Signing CA Public Key to ICAO, all receiving organisations 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 organisations.

A.Auth_PKI

The issuing and receiving organisations or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Protocol. The Organisation 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 Organisation Verifying Certification Authorities of the issuing organisations 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 organisations or Organizations. The issuing organisations or Organizations distribute the public keys of their Organisation Verifying Certification Authority to their MRD's chip.

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 MRD data in EF.DG1 to EF.DG24, the Document security object according to specifications [R2,R8] 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.DG2 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.

OT.Sens_Data_Conf

The TOE must ensure the confidentiality of the highly sensitive reference data 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 Organisation Verifier Certification Authority of the issuing organisation. The TOE must ensure the confidentiality of the logical MRD data during their transmission to the Extended Inspection System. The confidentiality of the highly sensitive 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).

OT.Chip_Auth_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 organisation by means of the Chip Authentication as defined in [R2]. The authenticity proof provided by 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 or (iv) bypass, dEAPtivate, 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 high 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-organisation 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 MRD'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 in [R1] as "Active Authentication".

5.2 Security objectives for the Operational Environment

5.2.1 Issuing organisation

The issuing organisation 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 rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

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

Procedures shall ensure that people (shipping department, carrier, 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 organisation must ensure that the Personalization Agents acting on behalf of the issuing organisation (i) establish the correct identity of the holder and create biographical data for the MRD, (ii) enroll the highly sensitive reference data of the MRD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (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 organisation must (i) generate a cryptographic secure Organisation Signing CA Key Pair, (ii) ensure the secrecy of the Organisation Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the

Certificate of the Organisation Signing CA Public Key to receiving organisations maintaining its authenticity and integrity. The issuing organisation 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 and (iii) distribute the Certificate of the Document Signer Public Key to receiving organisations. 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,R7].

OE.Auth_Key_MRD

The issuing organisation 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 and (iii) support inspection systems of receiving organisations 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 organisation has to establish the necessary public key infrastructure in order to limit the access to highly sensitive reference data of MRD's holders to authorized receiving organisations or Organizations. The Organisation Verifying Certification Authority of the issuing organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

OE.BAP-PP

It has to be ensured by the issuing organisation, that the TOE is additionally successfully evaluated and certified, based on "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control" [R10]. This is necessary to cover the BAP 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.

5.2.2 Receiving organisation

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

OE.Exam_MRD

The inspection system of the receiving organisation must examine the MRD presented by the holder 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 Organisation Signing CA Public Key and the Document Signer Public Key of each issuing organisation, and (ii) implements the terminal part of the Basic Access Protocol [R2]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRD's chip.

OE.Passive_Auth_Verif

The border control officer of the receiving organisation uses the inspection system to verify the holder 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 organisations must manage the Organisation Signing CA 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 organisation ensures the confidentiality and integrity of the data read from the logical MRD. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol.

OE.Ext_Insp_Systems

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

5.3 Security Objectives Rationale

5.3.1 Threats

T.Read_Sensitive_Data The threat T.Read_Sensitive_Data "Read the highly sensitive reference data" is countered by the TOE-objective OT.Sens_Data_Conf "Confidentiality of highly sensitive reference data" requiring that read access to DGs protected by EAP as specified in EF.COM (containing the highly sensitive reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data confidentiality. The authorization bases on Document Verifier certificates issued by the issuing organisation as required by OE.Authoriz_Sens_Data "Authorization for use of highly sensitive reference data". The Document Verifier of the receiving organisation has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the highly sensitive reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

T.Forgery The threat T.Forgery "Forgery of data on MRD's chip" addresses the fraudulent alteration of the complete stored logical MRD or any part of it. The security objective OT.AC_Pers "Access Control for Personalization of logical MRD' requires the TOE to limit the write access for the logical MRD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRD according the security objective OT.Data_Int "Integrity of personal data" and OT.Prot_Phys-Tamper "Protection against Physical Tampering". The examination of the presented MRD passport book according to OE.Exam_MRD "Examination of the MRD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRD. The TOE environment will

detect partly forged logical MRD data by means of digital signature which will be created according to OE.Pass_Auth_Sign "Authentication of logical MRD by Signature" and verified by the inspection system according to OE.Passive_Auth_Verif "Verification by Passive Authentication".

T.Counterfeit The threat T.Counterfeit "MRD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRD chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof?"roof of MRD?' chip authentication" using a authentication key pair to be generated by the issuing organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_Key_MRD "MRD Authentication Key". According to OE.Exam_MRD "Examination of the MRD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRD's chip.

This attack is also thwarted by active authentication proving the authenticity of the chip as required by OT.Chip_Authenticity "Protection against forgery" using a authentication key pair to be generated by the issuing organisation. The Public active Authentication Key has to be written into DG specified in EF.SOD and signed by means of Documents Security Objects.

T.Abuse-Func The threat T.Abuse-Func "Abuse of Functionality" addresses attacks using the MRD's chip as production material for the MRD and misuse of the functions for personalization in the operational organisation after delivery to MRD holder to disclose or to manipulate the logical MRD. This threat is countered by OT.Prot_Abuse-Func "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: OE.Personalization "Personalization of logical MRD' ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational organisation after delivery to MRD holder are enabled according to the intended use of the TOE.

The threat T.Abuse-Func?Abuse of Functionality? addresses attacks of misusing MRD?s functionality to disable or bypass the TSFs. The security objective for the TOE OT.Prot_Abuse- Func?Protection against abuse of functionality? ensures that the usage of functions which may not be used in the?Operational Use? phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE?s functions may be bypassed, dEAPtivated, changed or explored shall be effectively countered.

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

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

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

5.3.2 Organisational Security Policies

P.BAP-PP The OSP P.BAP-PP is directly addressed by the OE.BAP-PP.

P.Sensitive_Data The OSP P.Sensitive_Data "Privacy of highly sensitive reference data" is fulfilled by the TOE-objective OT.Sens_Data_Conf "Confidentiality of highly sensitive reference data" requiring that read access to DGs protected by EAP as specified in EF.COM (containing the highly sensitive reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data confidentiality. The authorization bases on Document Verifier certificates issued by the issuing organisation as required by OE.Authoriz_Sens_Data "Authorization for use of highly sensitive reference data". The Document Verifier of the receiving organisation has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the highly sensitive reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

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

P.Personalization The OSP P.Personalization "Personalization of the MRD by issuing organisation only" addresses the (i) the enrolment of the logical MRD by the Personalization Agent as described in the security objective for the TOE environment OE.Personalization "Personalization of logical MRD', and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers "Access Control for Personalization of logical MRD'. Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to OT.Identification "Identification and Authentication of the TOE". The security objective OT.AC_Pers limits the management of TSF data and management of TSF to the Personalization Agent.

P.Sensitive_Data_Protection The OSP P.Sensitive_data_Protection requires data to be protected in integrity as fullfilled by OT.Data_Int. Concerning keys, they must be protected in confidentiality in any cases as ensured by OT.Prot_Inf_Leak.

P.Key_Function The OSP P.Key_function requires cryptographic algorithms to be protected against tampering as it enforced for the whole TOE by OT.Prot_Phys-Tamper and also designed in order to avoid data leakage as ensured by OT.Prot_Inf_Leak.

5.3.3 Assumptions

A.MRD_Manufact The assumption A.MRD_Manufact "MRD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment OE.MRD_Manufact "Protection of the MRD Manufacturing" that requires to use security procedures during all manufacturing steps.

A.MRD_Delivery The assumption A.MRD_Delivery "MRD delivery during step 4 to 6" is covered by the security objective for the TOE environment OE.MRD_ Delivery "Protection of the MRD delivery" that requires to use security procedures during delivery steps of the MRD.

A.Pers_Agent The assumption A.Pers_Agent "Personalization of the MRD's chip" is covered by the security objective for the TOE environment OE.Personalization "Personalization of logical MRD' including the enrolment, the protection with digital signature and the storage of the MRD holder personal data.

A.Insp_Sys The examination of the MRD passport book addressed by the assumption A.Insp_Sys "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_MRD "Examination of the MRD passport book". The security objectives for the TOE environment OE.Prot_Logical_MRD "Protection of data from the logical MRD' will require the Basic Inspection System to implement the Basic Access Protocol and to protect the logical MRD data during the transmission and the internal handling.

A.Signature_PKI The assumption A.Signature_PKI "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Pass_Auth_Sign "Authentication of logical MRD by Signature" covering the necessary procedures for the Organisation Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_MRD "Examination of the MRD passport book".

A.Auth_PKI The assumption A.Auth_PKI "PKI for Inspection Systems" is covered by the security objective for the TOE environment OE.Authoriz_Sens_Data "Authorization for use of highly sensitive reference data" requires the True Root Certificate to limit the read access to highly sensitives by issuing Document Verifier certificates for authorized receiving organisations or Organizations only. The Document Verifier of the receiving organisation is required by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing organisation has to establish the necessary public key infrastructure.

5.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Read_Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 2.3.1
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRD, OE.Passive_Auth_Verif	Section 2.3.1
T.Counterfeit	OT.Chip_Auth_Proof, OT.Chip_Authenticity, OE.Auth_Key_MRD, OE.Exam_MRD	Section 2.3.1
T.Abuse-Func	OT.Prot_Abuse-Func	Section 2.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 2.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 2.3.1
T.Malfunction	OT.Prot_Malfunction	Section 2.3.1

Tableau 1 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.AC_Pers	T.Forgery
OT.Data_Int	T.Forgery
OT.Sens_Data_Conf	T.Read_Sensitive_Data
OT.Identification	
OT.Chip_Auth_Proof	T.Counterfeit
OT.Prot_Abuse-Func	T.Abuse-Func
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper
OT.Prot_Malfunction	T.Malfunction
OT.Chip_Authenticity	T.Counterfeit
OE.MRD_Manufact	
OE.MRD_Delivery	
OE.Personalization	
OE.Pass_Auth_Sign	T.Forgery
OE.Auth_Key_MRD	T.Counterfeit
OE.Authoriz_Sens_Data	T.Read_Sensitive_Data
OE.BAP-PP	
OE.Exam_MRD	T.Forgery, T.Counterfeit
OE.Passive_Auth_Verif	T.Forgery
OE.Prot_Logical_MRD	
OE.Ext_Insp_Systems	T.Read_Sensitive_Data

Tableau 2 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.BAP-PP	OE.BAP-PP	Section 2.3.2
P.Sensitive_Data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 2.3.2
P.Manufact	OT.Identification	Section 2.3.2
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization	Section 2.3.2
P.Sensitive_Data_Protection	OT.Data_Int, OT.Prot_Inf_Leak	Section 2.3.2
P.Key_Function	OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper	Section 2.3.2

Tableau 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.AC_Pers	P.Personalization
OT.Data_Int	P.Sensitive_Data_Protection
OT.Sens_Data_Conf	P.Sensitive_Data
OT.Identification	P.Manufact, P.Personalization
OT.Chip_Auth_Proof	
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	P.Sensitive_Data_Protection, P.Key_Function
OT.Prot_Phys-Tamper	P.Key_Function
OT.Prot_Malfunction	
OT.Chip_Authenticity	
OE.MRD_Manufact	
OE.MRD_Delivery	
OE.Personalization	P.Personalization
OE.Pass_Auth_Sign	
OE.Auth_Key_MRD	
OE.Authoriz_Sens_Data	P.Sensitive_Data
OE.BAP-PP	P.BAP-PP
OE.Exam_MRD	
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRD	
OE.Ext_Insp_Systems	P.Sensitive_Data

Tableau 4 Security Objectives and OSPs - Coverage

Assumptions	Security objectives for the Operational Environment	Rationale
A.MRD_Manufact	OE.MRD_Manufact	Section 2.3.3
A.MRD_Delivery	OE.MRD_Delivery	Section 2.3.3
A.Pers_Agent	OE.Personalization	Section 2.3.3
A.Insp_Sys	OE.Exam_MRD, OE.Prot_Logical_MRD	Section 2.3.3
A.Signature_PKI	OE.Pass_Auth_Sign, OE.Exam_MRD	Section 2.3.3
A.Auth_PKI	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	Section 2.3.3

Tableau 5 Assumptions and Security Objectives for the Operational Environment - Coverage

Security objectives for the Operational Environment	Assumptions
OE.MRD_Manufact	A.MRD_Manufact
OE.MRD_Delivery	A.MRD_Delivery
OE.Personalization	A.Pers_Agent
OE.Pass_Auth_Sign	A.Signature_PKI
OE.Auth_Key_MRD	
OE.Authoriz_Sens_Data	A.Auth_PKI
OE.BAP-PP	
OE.Exam_MRD	A.Insp_Sys, A.Signature_PKI
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRD	A.Insp_Sys
OE.Ext_Insp_Systems	A.Auth_PKI

Tableau 6 Security Objectives for the Operational Environment and Assumptions - Coverage

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

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

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

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].

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

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].

6.1.5 Extended family FIA_API - Authentication Proof of Identity

6.1.5.1 Description

See [R11]§5.3 for more details.

6.1.5.2 Extended components

Extended component FIA_API.1

Description

See [R11]§5.3 for more details.

Definition

FIA_API.1 Authentication Proof of Identity

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 [R11]§5.3 for more details.

6.1.5.3 Rationale

See [R11]§5.3 for more details.

7 Security Functional Requirements

7.1 Security Functional Requirements

Definitions of security attributes, keys and certificated referred in this section can be foun din [R11]§6.

7.1.1 PP EAP

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 **Diffie Hellman or Elliptic Curve Diffie Hellmann** and specified cryptographic key sizes **112 bits** that meet the following: **[R4], Annex A.1**.

FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384 ans SHA-512** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

FCS_COP.1/SYM Cryptographic operation

FCS_COP.1.1/SYM The TSF shall perform **secure messaging - encryption and decryption**

in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bits** that meet the following: **TR-03110 [R4]**.

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 **MAC Algo 3** and cryptographic key sizes **112 bits** that meet the following: **TR-03110 [R4]**.

FCS_COP.1/SIG_VER Cryptographic operation

FCS_COP.1.1/SIG_VER The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **RSASSA-PKCS1-v1_5 or RSASSA-PSS or ECDSA with SHA algorithms as specified in FCS_COP.1/SHA** and cryptographic key sizes

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

that meet the following:

- **[R24] and [R24] for RSASSA,**
- **[R17], [R18], [R19] for ECDSA**.

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_UID.1 Timing of identification

FIA_UID.1.1 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 carry out the Chip Authentication Protocol,**

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 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 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. Terminal Authentication Protocol,**
- **2. Authentication Mechanisms based on Triple-DES and AES**.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

- **1. Terminal Authentication Protocol,**
- **2. Secure messaging in MAC-ENC mode,**
- **3. 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**
  - **the Symmetric Authentication Mechanism with Personalization Agent Key,**
- **2. 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,**
- **3. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism**.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS**.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **Chip Authentication Protocol according to [R4]** to prove the identity of the **TOE**.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 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 and Active Authentication private key of the logical MRD**.

FDP_ACF.1 Security attribute based access control

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

- **1. Subjects:**
  - **a. Personalization Agent,**
  - **b. Extended Inspection System,**
  - **c. Terminal,**
- **2. Objects:**
  - **a. data EF.DG1 to EF.DG24 of the logical MRD,**
  - **b. data in EF.COM,**
  - **v. data in EF.SOD,**
  - **d. Active Authentication public key,**
- **3. Security attributes:**
  - **a. authentication status of terminals,**
  - **b. Terminal Authorization**.

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.DG24 of the logical MRD, including the Active Authenticate public Key,**
- **2. the successfully authenticated Extended Inspection System with the Read access to a higly senstive DG granted by the relative certificate holder**

authorization encoding is allowed to read the data in this DG of the logical MRD.

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. A terminal authenticated as True Root Certificate is not allowed to read data in an EF.DG protected by EAP as specified in EF.COM,**
- **2. A terminal authenticated as DV is not allowed to read data in EF.DG protected by EAP as specified in EF.COM,**
- **3. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG24 of the logical MRD,**
- **4. Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG protected by EAP as specified in EF.COM of the logical MRD**.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 [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**.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 [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**.

FDP_UIT.1.2 [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**.

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. Organisation Verifying Certification Authority,**
- **4. Document Verifier,**
- **5. Domestic Extended Inspection System,**
- **6. Foreign Extended 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 manipulated,**
- **2. highly sensitive User Data to be disclosed,**
- **3. TSF data to be disclosed or manipulated,**
- **4. software to be reconstructed and,**
- **5. 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 manipulated,**
- **2. Highly sensitive User Data to be disclosed,**
- **3. TSF data to be disclosed or manipulated,**
- **4. software to be reconstructed and,**
- **5. 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/True Root Certificate_INI Management of TSF data

FMT_MTD.1.1/True Root Certificate_INI The TSF shall restrict the ability to **write** the

- **1. initial Organisation Verifying Certification Authority Public Key,**
- **2. initial Organisation Verifying Certification Authority Certificate,**
- **3. initial Current Date**

to **the Personalization Agent**.

FMT_MTD.1/True Root Certificate_UPD Management of TSF data

FMT_MTD.1.1/True Root Certificate_UPD The TSF shall restrict the ability to **update** the

- **1. Organisation Verifying Certification Authority Public Key,**
- **2. Organisation Verifying Certification Authority Certificate**

to **Organisation Verifying Certification Authority**.

FMT_MTD.1/DATE Management of TSF data

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

- **1. Organisation Verifying Certification Authority,**
- **2. Document Verifier,**
- **3. domestic Extended Inspection System**.

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/CAPK Management of TSF data

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

FMT_MTD.1/KEY_READ Management of TSF data

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

- **1. Document Basic Access keys,**
- **2. Chip Authentication Private key,**
- **3. Personalization Agent Keys,**
- **4. Active Authentication private key**

to **none**.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 [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 Organisation 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 Organisation Verifying Certification Authority can be verified as correct with the public key of the Organisation Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Organisation Verifying Certification Authority is not before the Current Date of the TOE.

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

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

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **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 or any EF,**
- **Prior to any use of TSF data,**
- **Before execution of any command,**
- **When performing a BAP authentication,**
- **When using the True Root Certificate Root key,**
- **When verifying a certificate with an extracted public key µ,**
- **When performing the Chip Authentication,**
- **When performing a Terminal 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_MRD Cryptographic operation

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

- **1024 to 2048 bits for RSA CRT (by steps of 256bits),**
- **192, 256, 384 and 512 bits for ECDSA,**

that meet the following:

- **scheme 1 of [R20] for RSA CRT,**
- **[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 Protocol 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, 1536 and 2048 for RSA,**
- **192bits, 224bits, 256 bits, 384 bits and 512 bits over characteristic p curves for ECC**

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

7.1.3 Extended Access Protection (EAP)

FCS_CKM.1/EAP Cryptographic key generation

FCS_CKM.1.1/EAP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Diffie Hellman or Elliptic Curve Diffie Hellman** and specified cryptographic key sizes **128, 192 and 256 bits for the AES** that meet the following: **[R8], Annex C.1**.

FCS_COP.1/EAP-SM Cryptographic operation

FCS_COP.1.1/EAP-SM The TSF shall perform **secure messaging - encryption, decryption and message authentication code**

in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128, 192 and 256 bits** that meet the following: **FIPS 197 [R30]**.

7.2 Security Assurance Requirements

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

7.3 Security Requirements Rationale

7.3.1 Objectives

7.3.1.1 Security Objectives for the TOE

OT.AC_Pers The security objective OT.AC_Pers "Access Control for Personalization of logical MRD" addresses the access control of the writing the logical MRD. The write access to the logical MRD data are defined by the SFR FIA_UID.1, FIA_UAU.1, FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG24 of the logical MRD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Protocol.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/EAP, FCS_COP.1/EAP-SM, FCS_CKM.1, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6 (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMS.1 the confidentially of these keys.

OT.Data_Int The security objective OT.Data_Int "Integrity of personal data" requires the TOE to protect the integrity of the logical MRD stored on the MRD's chip against physical manipulation and unauthorized writing. The write access to the logical MRD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG24 of the logical MRD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG24 of the logical MRD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1 and FIA_UAU.1 before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6. The SFR FIA_UAU.6 and FDP_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by

the cryptographic functions according to FCS_CKM.1 and FCS_CKM.1/EAP (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/EAP-SM, FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

OT.Sens_Data_Conf The security objective OT.Sense_Data_Conf "Confidentiality of highly sensitive reference data" is enforced by the Access Control SFP defined in FDP_ACC.1 and FDP_ACF.1 allowing the data of DGs protected by EAP as specified in EF.COM only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS_COP.1/SIG_VER.

The SFR FIA_UID.1 and FIA_UAU.1 requires the identification and authentication of the inspection systems. The SFR FIA_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4.The SFR FIA_UAU.6 and FDP_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1 and FCS_CKM.1/EAP (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/EAP-SM, FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the True Root Certificate's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/True Root Certificate_INI, FMT_MTD.1/True Root Certificate_UPD and FMT_MTD.1/DATE.

OT.Identification The security objective OT.Identification "Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification.

OT.Chip_Auth_Proof The security objective OT.Chip_Auth_Proof "Proof of MRD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1 and FCS_CKM.1/EAP is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol [R4] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/EAP-SM, FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

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

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

- 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, which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

OT.Prot_Malfunction The security objective OT.Prot_Malfunction "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure organisation in case of detected failure or operating conditions possibly causing a malfunction.

OT.Chip_Authenticity The security objective OT.Chip_Authenticity "Protection against forgery" is ensured by the Active Authentication Protocol activated by FMT_MOF.1/AA and provided by FDP_DAU.1/AA, FDP_ACC.1 and FDP_ACF.1 proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/SIG_MRD, FCS_COP.1/SHA and FCS_RND.1. It is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ, this key being loaded during personalization phase as required by FDP_ITC.1/AA or generated on-card by FCS_CKM.1/ASYM.

7.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.AC_Pers	FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/MAC, FCS_RND.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FPT_EMS.1, FCS_COP.1/SYM, FCS_COP.1/SIG_VER, FIA_UID.1, FIA_UAU.1, FCS_CKM.1/EAP, FCS_COP.1/EAP-SM	Section 4.3.1
OT.Data_Int	FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/MAC, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_READ, FCS_CKM.4, FCS_COP.1/SYM, FIA_UID.1, FIA_UAU.1, FMT_MTD.1/CAPK, FCS_CKM.1/EAP, FCS_COP.1/EAP-SM	Section 4.3.1
OT.Sens_Data_Conf	FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/MAC, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FMT_MTD.1/KEY_READ, FCS_COP.1/SYM, FCS_COP.1/SIG_VER, FMT_MTD.1/True Root Certificate_INI, FMT_MTD.1/True Root Certificate_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.3, FCS_CKM.1/EAP, FCS_COP.1/EAP-SM	Section 4.3.1

Security Objectives	Security Functional Requirements	Rationale
OT.Identification	FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS	Section 4.3.1
OT.Chip_Auth_Proof	FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_CKM.1/EAP, FCS_COP.1/EAP-SM	Section 4.3.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 4.3.1
OT.Prot_Inf_Leak	FPT_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3	Section 4.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 4.3.1
OT.Prot_Malfunction	FPT_FLS.1, FPT_TST.1	Section 4.3.1
OT.Chip_Authenticity	FCS_CKM.1/ASYM, FCS_COP.1/SHA, FCS_RND.1, FDP_DAU.1/AA, FDP_ACC.1, FDP_ACF.1, FDP_ITC.1/AA, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FCS_COP.1/SIG_MRD, FMT_MOF.1/AA	Section 4.3.1

Tableau 7 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FAU_SAS.1	OT.Identification
FCS_CKM.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_CKM.4	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FCS_COP.1/SHA	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Chip_Authenticity
FCS_COP.1/SYM	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/MAC	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/SIG_VER	OT.AC_Pers, OT.Sens_Data_Conf
FCS_RND.1	OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Authenticity
FIA_UID.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.4	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.5	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_UAU.6	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf
FIA_API.1	OT.Chip_Auth_Proof
FDP_ACC.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Authenticity
FDP_ACF.1	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Authenticity
FDP_UCT.1	OT.Sens_Data_Conf
FDP_UIT.1	OT.Data_Int
FMT_SMF.1	OT.AC_Pers, OT.Data_Int
FMT_SMR.1	OT.AC_Pers, OT.Data_Int
FMT_LIM.1	OT.Prot_Abuse-Func
FMT_LIM.2	OT.Prot_Abuse-Func
FMT_MTD.1/INI_ENA	OT.Identification

Security Functional Requirements	Security Objectives
FMT_MTD.1/INI_DIS	OT.Identification
FMT_MTD.1/True Root Certificate_INI	OT.Sens_Data_Conf
FMT_MTD.1/True Root Certificate_UPD	OT.Sens_Data_Conf
FMT_MTD.1/DATE	OT.Sens_Data_Conf
FMT_MTD.1/KEY_WRITE	OT.AC_Pers, OT.Chip_Authenticity
FMT_MTD.1/CAPK	OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FMT_MTD.1/KEY_READ	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Chip_Authenticity
FMT_MTD.3	OT.Sens_Data_Conf
FPT_EMS.1	OT.AC_Pers, OT.Prot_Inf_Leak
FPT_FLS.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_TST.1	OT.Prot_Inf_Leak, OT.Prot_Malfunction
FPT_PHP.3	OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper
FDP_DAU.1/AA	OT.Chip_Authenticity
FCS_COP.1/SIG_MRD	OT.Chip_Authenticity
FDP_ITC.1/AA	OT.Chip_Authenticity
FMT_MOF.1/AA	OT.Chip_Authenticity
FCS_CKM.1/ASYM	OT.Chip_Authenticity
FCS_CKM.1/EAP	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof
FCS_COP.1/EAP-SM	OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof

Tableau 8 SFRs and Security Objectives

7.3.3 Dependencies

7.3.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/SYM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SIG_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_RND.1	No dependencies	
FIA_UID.1	No dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_API.1	No dependencies	
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1
FDP_UCT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1

Requirements	CC Dependencies	Satisfied Dependencies
FDP_UIT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_LIM.1	(FMT_LIM.2)	FMT_LIM.2
FMT_LIM.2	(FMT_LIM.1)	FMT_LIM.1
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/True Root Certificate_INI	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/True Root Certificate_UPD	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/DATE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CAPK	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1/True Root Certificate_INI, FMT_MTD.1/True Root Certificate_UPD
FPT_EMS.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	
FDP_DAU.1/AA	No dependencies	
FCS_COP.1/SIG_MRD	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4, FDP_ITC.1/AA, FCS_CKM.1/ASYM
FDP_ITC.1/AA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACC.1

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MOF.1/AA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FCS_CKM.1/ASYM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/SIG_MRD
FCS_CKM.1/EAP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/EAP-SM
FCS_COP.1/EAP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4

Tableau 9 SFRs dependencies

Rationale for the exclusion of dependencies

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is unsupported. The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

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

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

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

The dependency FMT_MSA.3 of FDP_ITC.1/AA is unsupported. FMT_MSA.3 dependency is not required since this import does not involve any specific security attribute.

7.3.3.2 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies	

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

Tableau 10 SARs dependencies

7.3.4 Rationale for the Security Assurance Requirements

This Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.

The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen

for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

7.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

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

All these dependencies are satisfied by EAL5.

7.3.6 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL5 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC_DVS.2 has no dependencies.

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 organisation.

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

- BAP keys,
- Chip authentication keys,
- True Root Certificate 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 as specified in EF.COM, the Document Security Object, the EF.True Root Certificate, EF.COM only after BAP authentication and throught a valid secure channel,
- When the EAP was successfully performed, The terminal can only read the DGs protected by EAP as specified in EF.COM, provided the access rights are sufficient throught 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 organisation.

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,
- the Root True Root Certificate key files and temporary key files are updated internally by the application according to the authentication mechanism described in [R4].

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).

EAC mechanism

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

- it handles the certificate verification,
- the management of access rights to higly sensitive DGs as specified in EF.COM,
- 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 True Root Certificate 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.

EAP mechanism

This security functionality enforce EAP by providing generation of AES keys and support of AES Secure Messaging as described in Security functionnality "Secure Messaging".

Secure Messaging

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

After a successful BAP authentication and successful Chip authentication, a secure channel is (re)established based on Triple DES or AES 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 BAP or EAP).

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 [R1] & [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 BAP and Active Authentication,
- Self tests of the DES before the BAP,
- 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 organisation management

This security functionalities ensures that the TOE gets bask to a secure organisation 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 organisation "kill card" or becomes mute.

Physical protection

This security functionality protects the TOE against physical attacks.

8.2 SFRs and TSS

8.2.1 SFRs and TSS - Rationale

8.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	Access Control in reading, Access Control in writing
FCS_CKM.1	EAC mechanism
FCS_CKM.4	EAC mechanism, Secure Messaging
FCS_COP.1/SHA	EAC mechanism
FCS_COP.1/SYM	Secure Messaging
FCS_COP.1/MAC	Secure Messaging
FCS_COP.1/SIG_VER	EAC mechanism
FCS_RND.1	Access Control in reading, EAC mechanism, Active Authentication
FIA_UID.1	EAC mechanism, Personalisation Agent Authentication
FIA_UAU.1	EAC mechanism, Active Authentication
FIA_UAU.4	EAC mechanism, Personalisation Agent Authentication
FIA_UAU.5	EAC mechanism, Secure Messaging, Personalisation Agent Authentication
FIA_UAU.6	Secure Messaging
FIA_API.1	EAC mechanism
FDP_ACC.1	Access Control in reading, Access Control in writing
FDP_ACF.1	Access Control in reading, Access Control in writing
FDP_UCT.1	Secure Messaging
FDP_UIT.1	Secure Messaging
FMT_SMF.1	Access Control in writing
FMT_SMR.1	Access Control in writing, Personalisation Agent Authentication, Secure Messaging, EAC mechanism
FMT_LIM.1	Access Control in reading, Self tests, Physical protection
FMT_LIM.2	Access Control in reading, Self tests, Physical protection
FMT_MTD.1/INI_ENA	Access Control in writing
FMT_MTD.1/INI_DIS	Access Control in writing
FMT_MTD.1/True Root Certificate_INI	Access Control in writing

Security Functional Requirements	TOE Summary Specification
FMT_MTD.1/True Root Certificate_UPD	Access Control in writing
FMT_MTD.1/DATE	Access Control in writing
FMT_MTD.1/KEY_WRITE	Access Control in writing
FMT_MTD.1/CAPK	Access Control in writing
FMT_MTD.1/KEY_READ	Access Control in reading
FMT_MTD.3	EAC mechanism
FPT_EMS.1	Access Control in reading, Access Control in writing, EAC mechanism, Secure Messaging, Personalisation Agent Authentication, Active Authentication, Physical protection
FPT_FLS.1	Safe organisation management
FPT_TST.1	Self tests
FPT_PHP.3	Physical protection
FDP_DAU.1/AA	Active Authentication
FCS_COP.1/SIG_MRD	Active Authentication
FDP_ITC.1/AA	Access Control in writing, Active Authentication
FMT_MOF.1/AA	Active Authentication, Access Control in writing
FCS_CKM.1/ASYM	Active Authentication
FCS_CKM.1/EAP	EAP mechanism
FCS_COP.1/EAP-SM	EAP mechanism

Tableau 11 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
Access Control in reading	FAU_SAS.1, FCS_RND.1, FDP_ACC.1, FDP_ACF.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/KEY_READ, FPT_EMS.1
Access Control in writing	FAU_SAS.1, FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/True Root Certificate_INI, FMT_MTD.1/True Root Certificate_UPD, FMT_MTD.1/DATE, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FPT_EMS.1, FDP_ITC.1/AA, FMT_MOF.1/AA
EAC mechanism	FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SIG_VER, FCS_RND.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_API.1, FMT_SMR.1, FMT_MTD.3, FPT_EMS.1
EAP mechanism	FCS_CKM.1/EAP, FCS_COP.1/EAP-SM
Secure Messaging	FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_UAU.5, FIA_UAU.6, FDP_UCT.1, FDP_UIT.1, FMT_SMR.1, FPT_EMS.1
Personalisation Agent Authentication	FIA_UID.1, FIA_UAU.4, FIA_UAU.5, FMT_SMR.1, FPT_EMS.1
Active Authentication	FCS_RND.1, FIA_UAU.1, FPT_EMS.1, FDP_DAU.1/AA, FCS_COP.1/SIG_MRD, FDP_ITC.1/AA, FMT_MOF.1/AA, FCS_CKM.1/ASYM
Self tests	FMT_LIM.1, FMT_LIM.2, FPT_TST.1
Safe organisation management	FPT_FLS.1
Physical protection	FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_PHP.3

Tableau 12 TSS and SFRs - Coverage

9 PP

9.1 PP reference

The ST is based on PP EAC in CC3.1 [R11].

For consistency reasons, editorial modifications have been performed:

- EAC replaced by EAP,
- MRTD replaced by MRD,
- “DG1 to DG16“ replacted by “DG1 to DG24”,
- State replaced by organization,
- MRZ replaced by keydoc,
- CVCA replaced by True Root Certificate,
- Reference to EF.COM for access control rules (which specifies which DG is protected by BAP or EAP). This implies especially the usage of the more general sentence “DGs protected by EAP as specified by EF.COM” instead of “DG3 and DG4”.

9.2 PP additions

The additional functionalities are the Active Authentication (AA) based on the ICAO PKI V1.1, the related on-card generation of RSA and ECC keys and the AES secure messaging following EAP. It implies some addition to the standard PP.

The following SFRs are added to the standard PP for the AA feature:

- FCS_COP.1 / SIG_MRTD
- FDP_DAU.1 / AA
- FDP_ITC / AA
- FMT_MOF.1 / AA
- FCS_CKM.1 / ASYM

The following SFR are added to the standard PP for the EAP feature:

- FCS_CKM.1 / EAP
- FCS_COP.1 / EAP-SM

The following Objective for the TOE is added to the standard PP for the AA feature:

- OT.Chip_authenticity “Protection against forgery”

Moreover, the composition with the IC mandates to introduce complementary OSPs:

- P.Sensitive_Data_Protection “Protection of sensitive data”
- P.Key_Function “Design of the cryptographic routines in order to protect the keys”

10 Composition with IC Security Target

IC Elements	Relevant	Consistent in ST with	Justification
A.Process-Sec-IC	Yes	P.Manufact	Security procedures are used during TOE packaging, finishing and pre-personalisation (During Phase 2)
A.Plat-Appl	No	n/a	This assumption deals with the development process and is therefore covered by the evaluation
A.Resp-Appl	Yes	P.Sensitive_Data_Protection	The Composite TOE ensure the confidentiality of the cryptographic keys it stores
A.Check-Init	Yes	P.Manufact	ICs are actually identified uniquely
A.Key-Function	Yes	P.Key_Function	The Cryptographic routines are designed in such a way that they do not compromise key by any leak of information
P.Add-Components	Yes	P.Sensitive_Data_Protection	The TOE ensure protection of data using especially the 3DES and AES algorithms
T.Leak-Inherent	Yes	(1)	(1)
T.Phys-Probing	Yes	(1)	(1)
T.Malfunction	Yes	(1)	(1)
T.Phys-Manipulation	Yes	(1)	(1)
T.Leak-Forced	Yes	(1)	(1)
T.Abuse-Func	Yes	(1)	(1)
T.RND	Yes	(1)	(1)
OE.Plat-Appl	No	n/a	This assumption deals with the development process and is therefore covered by the evaluation
OE.Resp-Appl	Yes	P.Sensitive_Data_Protection	The Composite TOE ensure the confidentiality of the cryptographic keys it stores as well as the integrity of all the sensitive data.

IC Elements	Relevant	Consistent in ST with	Justification
OE.Process-Sec-IC	Yes	P.Manufact	This objective is ensured by the security procedures and manufacturing guidelines of NXP manufacturing site
OE.Check-Init	Yes	P.Manufact	ICs are actually identified uniquely
O.Leak-Inherent	Yes	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper	Software is designed to be protected against leakage with the hardware support
O.Phys-Probing	Yes	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper	Objective require that memory and execution cannot be probed
O.Malfunction	Yes	OT.Prot_Malfunction	Correct operation of the TOE is controlled and malfunctions are detected
O.Phys-Manipulation	Yes	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper	Manipulation of the memory and the execution is controlled by the software. This is achieved with the hardware support
O.Leak-Forced	Yes	OT.Prot_Inf_Leak OT.Prot_Phys_Tamper	Software is designed to be protected against leakage with the hardware support
O.Abuse-Func	Yes	OT.Prot_Abuse-Func	Improper usage of the TOE is controlled
O.Identification	Yes	OT.Identification	Identification is fully handled during whole lifecycle of the TOE from IC manufacturing to use phase.
O.RND	Yes	OT.AC_Pers OT.Data_Int OT_Data_Conf	The Cryptographic routines are designed in such a way that they do not compromise random values in order to ensure confidentially, integrity and proof of origin.
O.HW_DES3	Yes	OT.AC_Pers OT.Data_Int OT_Data_Conf	3DES algorithm is used to enforce data integrity, data confidentiality and authentications.
O.HW_AES	Yes	OT.AC_Pers OT.Data_Int OT_Data_Conf	AES algorithm is used to enforce data integrity, data confidentiality and authentications.

IC Elements	Relevant	Consistent in ST with	Justification
O.MF_HW	No	n/a	Mifare is not supported
O.MEM_ACCESS	No	n/a	Not used.
O.SFR_ACCESS	No	n/a	Not used.
FRU_FLT.2	Yes	(2)	(2)
FPT_FLS.1	Yes	(2)	(2)
FMT_LIM.1	Yes	(2)	(2)
FMT_LIM.2	Yes	(2)	(2)
FAU_SAS.1	Yes	(2)	(2)
FPT_PHP.3	Yes	(2)	(2)
FDP_ITT.1	Yes	(2)	(2)
FPT_ITT.1	Yes	(2)	(2)
FDP_IFC.1	Yes	(2)	(2)
FCS_RNG.1	Yes	(2)	(2)
FCS_COP.1[DES]	Yes	(2)	(2)
FCS_COP.1[AES]	Yes	(2)	(2)
FDP_ACC.1[MEM]	Yes	(2)	(2)
FDP_ACC.1[SFR]	Yes	(2)	(2)
FDP_ACF.1[MEM]	Yes	(2)	(2)
FDP_ACF.1[SFR]	Yes	(2)	(2)
FMT_MSA.3[MEM]	Yes	(2)	(2)
FMT_MSA.3[SFR]	Yes	(2)	(2)
FMT_MSA.1[MEM]	Yes	(2)	(2)
FMT_MSA.1[SFR]	Yes	(2)	(2)
FMT_SMF.1	Yes	(2)	(2)

(1) Since IC objectives are consistent with TOE objectives, IC Threats are also consistent with TOE SPD
(2) Since IC SFRs are translations of IC objectives, IC SFRs are consistent with TOE SFRs

11 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-2009-07-001, version 3.1 Revision 3 Final, July 2009

[R34] Common Criteria for Information Technology security Evaluation Part 2 : Security Functional Components, CCMB-2009-07-002, version 3.1 Revision 3 Final, July 2009

[R35] Common Criteria for Information Technology security Evaluation Part 3 : Security Assurance Components, CCMB-2009-07-003, version 3.1 Revision 3 Final, July 2009

12 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
MRD	Machine readable 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

T