e-Passport AXSEAL CC V2 72K

Common Criteria / ISO15408

EAL4 +

Security target Public Version

AXSEAL V2 CC 72K SECURITY TARGET (PUBLIC VERSION)
HERMES PROJECT

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: AXSEAL CC V2 72K Security Target (public version)

Version: V1.4 issued October 2006

ST reference: D1033361

Origin: Gemalto

Product identification: AXSEAL V2 CC 72K

Product under evaluation (PUE) reference:

Revision of the certified IC on which the software is embedded: P5CD072 V0Q

IC Certificate Reference: BSI-DSZ-CC-0349-2006

Manufacturing identification: Part A1002922 (CHIP M576ICAOP3M P5CD072V3 MOB4)

The content of this public security target is equivalent to the version 1.4, only some chapters have been removed for confidentiality reasons

TOE identification :

The TOE is uniquely identified by following data:

Field	Length	Meaning / Value	Location
IC Fabricator	2	Philips / 40 70	EEPROM
IC Type	2	P5CD072V0Q / 00 15	EEPROM
Operating System identifier	3	D0 00 42	EEPROM
Non volatile memory embedded software identifier (Softmask)	2	Softmask number - Softmask version (0000 if no softmask loaded)	OTP

Table 1-1. TOE identification data

The TOE identification data are located in EEPROM area and in OTP (One Time Programming) memory (written during pre-personalization phase). These data are available by executing an administrative command (see [ADM]).

TOE Software identification:

In the Omniworks software configuration management system, the TOE software is uniquely identified by the actual configuration revision number 456.

Softmask identification: In case a softmask is loaded, it will also be uniquely identified by the actual configuration revision number.

1.2 ST OVERVIEW

This Security Target defines the security requirements for the AXSEAL product. This product is a new product based on secure operating system addressing the Machine Readable Travel Document (MRTD) applications. Specifications and requirements are issued by the International Civil Aviation Organization (ICAO).

The Machine Readable Travel Document is a passport which embeds the AXSEAL product composed of a contact-less interface integrated circuit with a dedicated software and an antenna. The AXSEAL product ensures the authentication of the passport holder through Basic Access Control and chip authenticity proof by means of Active Authentication. Additionally the AXSEAL product provides personalization and administration services to the Issuing States or Organizations.

The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the MRTD application and data during its life cycle.

The main objectives of this ST are:

- To introduce AXSEAL product and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.
- To give a rational for this ST.
- To show how the security functions provided by the integrated circuit are supporting the security requirements of the TOE.

1.3 CC CONFORMANCE

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, January 2004, version 2.2, CCIMB-2004-01-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, January 2004, version 2.2, CCIMB-2004-01-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, January 2004, version 2.2, CCIMB-2004-01-003,

including the

- Final Interpretation of CCIMB as of 04.04.2005,

as follows

- Part 2 extended,,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2 and ALC_DVS.2.

1.4 REFERENCES

1.4.1 External References

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCIMB-2004-01-001, version 2.2, January 2004
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-2004-01-002, version 2.2, January 2004
[CC-3]	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-2004-01-003, version 2.2, January 2004
[CEM]	Common Methodology for Information Technology Security Evaluation CCIMB-2004-01-004, version 2.2, January 2004.
[MRTD-PP]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0017, version 1.0, 18 August 2005
[ST-PHILIPS]	Security Target Lite, P5CT072V0Q/P5CD072V0Q/P5CD036V0Q Secure Smart Card Controller BSI-DSZ-CC-0349, version 1.2, Philips Semiconductors, 13 January 2006
[GDO-PHILIPS]	Guidance, Delivery and Operation Manual for the P5CT072V0Q/P5CD072V0Q/P5CD036V0Q, Version 1.1, Philips Semiconductors, 13 January 2006
[DS-PHILIPS]	Data Sheet, P5CD072 V0P/V0Q, SmartMX, Secure Dual Interface Smart Card Controller, Objective Specification, Philips Semiconductors, Revision 2.0, September 14th, 2005
[IS-PHILIPS]	Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, Philips Semiconductors, Revision 1.0, May 09, 2003
[AN-PHILIPS]	Contactless operation on SmartMX P5CDxxx/ P5CTxxx devices, Application note, Philips Semiconductors, Revision 1.0, September 2005
[SSVGPP]	Smartcard IC Platform protection Profile BSI-PP-0002, version 1.0, July 2001
[LDS]	MRTD Technical Report, Development of a Logical Data Structure LDS for optional capacity technologies Technical Report, International Civil Aviation Organization LDS 1.7 -2004-05-18, revision 1.7, May 2005
[PKI]	MRTD Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access Technical Report, International Civil Aviation Organization Version 1.1, October 2004
[ASM]	Advanced Security Mechanisms for Machine Readable Travel Documents Technical Report, Bundesamt für Sicherheit in der Informationstechnik Version 0.85

[SS]	ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 Machine Readable Passports, Fifth Edition – 2003
[BIO]	BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004
[SUP]	Supplement ICAO Doc 9303, Machine Readable Passports, V3.0, 12 June 2005
[CIC]	Annex I, Use of Contactless Integrated Circuit in Machine Readable Documents Version 4.0, ICAO TAG MRTD/NTWG, 5 May 2004
[ISO]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS2004

1.4.2 Internal References

[IGS]	Installation, Generation and Start Up Procedures, D1028644
[ADM]	Administrator Guidance, D1028647
[USR]	User Guidance, D1028648

1.5 ACRONYMS AND GLOSSARY

Acr.	Term	Definition
AA	Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
	Application note [MRTD-PP]	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
	Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
	Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
BIS	Basic Inspection System	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
	Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [SS]
	Biometric Reference Data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
	Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [SS]
CCSCA	Country Signing CA Certificate	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
	Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key $_{KENC)}$ and message authentication (key $_{KMAC)}$ of data transmitted between the MRTD's chip and the inspection system [PKI]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
SOD	Document Security Object	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [PKI]
	Eavesdropper	A threat agent with moderate attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
	Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [BIO]

EAC	Extended Access Control	Security mechanism identified in [PKI] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
EIS	Extended Inspection System	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
	Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [BIO]
	IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
	IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
	Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [SS]
	Improperly	A person who travels, or attempts to travel with: (a) an expired travel
	Documented person	document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [BIO]
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
	Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [BIO]
IS	Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
	Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
	Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [LDS]

	Issuing State	The Country issuing the MRTD. [LDS]
LDS	Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [LDS]. The capacity expansion technology used is the MRTD's chip.
	Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [LDS] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, DG1), (2) the digitized portraits (DG2), (3) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (4) the other data according to LDS (DG5 to DG16).
	Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
MRTD	Machine readable travel document	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [LDS]
MRV	Machine readable visa	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [LDS]
MRZ	Machine Readable Zone	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [LDS]
	Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [SS]
	MRTD administrator	The Issuing State or Organization which is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.
	MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: - -the file structure implementing the LDS [LDS], - the definition of the User Data, but does not include the User Data itself (i.e. content of DG1 to DG14 and DG 16), - - the TSF Data including the definition the authentication data but except the authentication data itself.
	MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
	MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
	MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and ICAOT, [10], p. 14. programmed according to the Logical Data Structure as specified by ICAOT, [10], p. 14.
	MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.

	Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
	Passive authentication	- verification of the digital signature of the Document Security Object - comparison the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
	Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
	Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
	Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
	Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
	Pre –personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
PIS	Primary Inspection System	A inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
	Receiving State	The Country to which the MRTD holder is applying for entry. [LDS]
	reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
	secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [SS]
	secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4

	Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
	travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. [BIO]
	traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
	Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
	User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
	Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [BIO]
	verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

1.6 APPLICATION NOTE USE AND PP OPTION

Application notes issued from the protection profile [MRTD-PP] are copied in this security target without modification and are written in the following way: *Application note [MRTD-PP].*

Application notes dedicated to this security target are specified as: *Application note [ST].*

Some parts of the PP are not applicable to the product specified in this ST as the PP includes 2 options for the product specification (no-BAC mode and BAC mode) In this case the non-relevant paragraphs are annotated as: *Not Applicable to this ST* or an application note details the differences.

2. TOE DESCRIPTION

2.1 TOE BOUNDARIES

Application note [ST]: The final product is a MRTD passport including a coversheet. A contactless integrated circuit connected to an antenna is mounted on a plastic film. This film is then embedded in the coversheet of the MRTD passport and provides a contactless interface for the passport holder identification.

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

- the Basic Access Control (BAC) according to the ICAO document [PKI].

Application note [ST]: Additionally to the [MRTD-PP], following functionalities are also provided:

- the Active Authentication mechanism [PKI],
- a set of administrative commands for the management of the product during the product life.

The TOE comprises of:

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and the associated guidance documentation.

Application note [ST]: Components within the TOE boundary are refined in the following manner:

- the Integrated Circuit (IC) Philips P5CD072 V0Q,
- the IC Dedicated Test Software,
- the IC Dedicated Support Software (Boot Rom Software, Mifare Operating System),
- the hardware for the contactless interface (e.g. antenna),
- the AXSEAL Embedded Software (ES),
- the NVM Embedded Software (if any),
- part of the MRTD Logical Data Structure,
- the guidance documentation of the AXSEAL product:
    - the administrator's guide [AGD-ADM],
    - the user's guide [AGD-USR].

The AXSEAL V2CC Embedded Software (AXSEAL V2CC ES) is implemented in the ROM of the chip. This AXSEAL V2CC ES provides mechanisms to load executable code into the non-volatile-memory of the chip (EEPROM). These mechanisms are included in the TOE and are part of the evaluation.

The TOE is delivered to the Personalization Agents with data and guidance documentation in order to perform the personalization of the product according to Figure 2.3.

2.2 TOE INTENDED USAGE

State or organization issues MRTD to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity.

The MRTD in context of this security target contains:

- visual (eye readable) biographical data and portrait of the holder,
- a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ),
- data elements on the MRTD's chip according to LDS for contactless machine reading.

The authentication of the traveler is based on the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of:

- the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:
  - the biographical data on the biographical data page of the passport book,
  - the printed data in the Machine-Readable Zone (MRZ),
  - the printed portrait.
- the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [LDS] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder:
  - the digital Machine Readable Zone Data (digital MRZ data, DG1),
  - the digitized portraits (DG2),
  - the optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both,
  - the other data according to LDS (DG5 to DG16),
  - the Document security object,
  - the file structure and dedicated files (e.g. EF.DIR) required for the product management.

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

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

2.3 IT FEATURES OF THE TOE

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access

Control to and the Data Encryption of additional biometrics as optional security measure in the ICAO Technical report [PKI]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism.

The Basic Access Control is a security feature which shall be mandatory supported by the TOE. The inspection system (i) reads the printed data in the MRZ, (ii) authenticates themselves as inspection system by means of keys derived from MRZ data (Document Basic Access Keys). After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [PKI], Annex E, and [LDS].

Application note [ST]: Additionally to the PP, this security target addresses the Active Authentication: the Active Authentication mechanism is a security feature that may be performed (when MRTD with the optional DG15 is available to the inspection system) to ensure that the data is read from the genuine chip and that the chip and data page belong to each other.

Application note [ST]: Administration commands are also provided by the TOE during the use phase. By mean of an administration terminal, the TOE administrator may for example terminate the ICAO application and thus invalidate the passport.

Application note [ST]: The Basic Access Control cannot be disabled. The mode without Basic Access Control described in the [MRTD-PP] is not applicable to this ST.

2.4 SCOPE OF THE TOE

2.4.1 Physical scope of the TOE

Figure 2-1 displays a picture of the AXSEAL product embedded in the coversheet of a MRTD (Note: the design of the antenna is not contractual and could evolve during the product life).

The physical scope of the TOE could be represented by the AXSEAL product. (see Figure 2-1 below), which comprises the plastic film with the antenna and the chip.

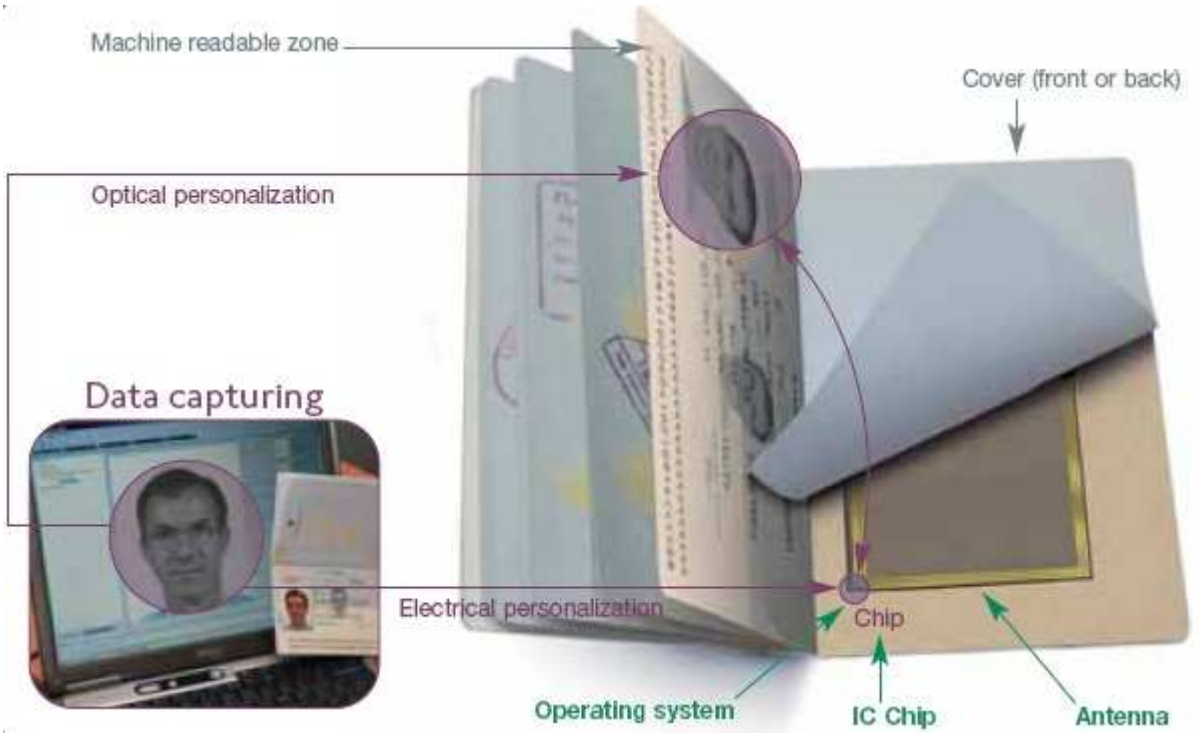


Figure 2-1.Physical aspect of the TOE embedded in the MRTD environment

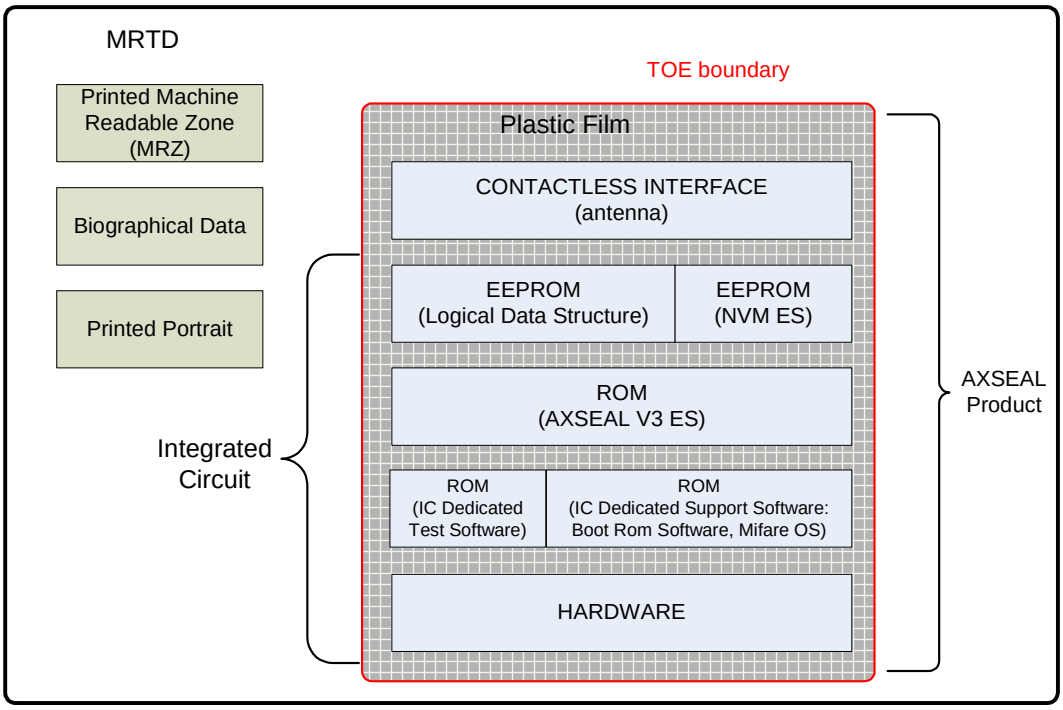


Figure 2-2. Physical structure of the TOE

2.4.2 Logical scope of the TOE

Figure 2-3 shows the logical file structure during operational use of the AXSEAL product. The file structure at TOE delivery is bordered with a red line. Only MF and Issuer Application DF are created. All EF files are created after TOE delivery by the Personalizer.

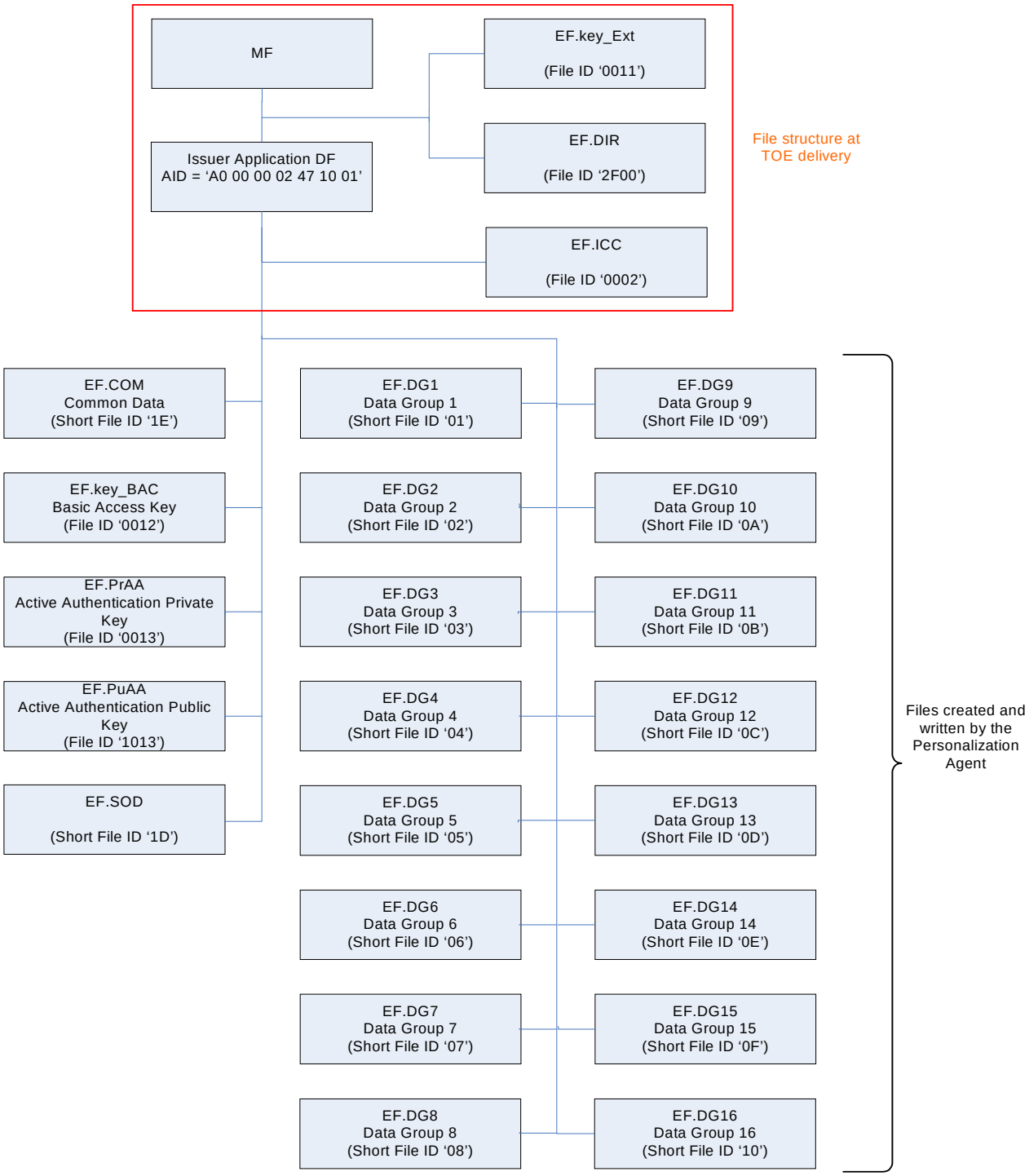


Figure 2-3: Logical data structure of the AXSEAL product

According to the issuing Organizations or States, some files are not mandatory (see Table 2-4 and [LDS]).

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/Integrity object (Security Object Document) is recorded within a separate elementary file (EF.SOD). A *mandatory* Header and Data Group Presence Map are included within each implementation method, this information is stored in EF.COM.

Data Group	Mandatory (M) / Optional (O)	Data Item
Detail (s) Recorded in MRZ of the MRTD		
1	M	Machine Readable Zone (MRZ) Data
Machine Assisted Identity Confirmation Detail (s) – Encoded Identification Feature (s)		
2	M	Global Interchange feature – Encoded Face
3	O	Additional Feature – Encoded Finger (s)
4	O	Additional Feature – Encoded Iris (s)
Machine Assisted Identity Confirmation Detail (s) – Displayed Identification Feature (s)		
5	O	Displayed Portrait
6	O	Reserved for future use
7	O	Displayed Signature or Usual Mark
Machine Assisted Security Feature Verification – Encoded Security Feature (s)		
8	O	Data Feature (s)
9	O	Structure Feature (s)
10	O	Substance Feature (s)
Additional Personal Detail (s)		
11	O	Additional Personal Data Elements
Additional Document Detail (s)		
12	O	Additional Document Data Elements
Optional Detail (s)		
13	O	Discretionary Data Element(s) defined by issuing State or Organization
Reserved for Future Use		
14	O	Reserved for future use
15	O	Active Authentication Public Key Info
Person (s) to Notify		
16	O	Person (s) to Notify Data Element(s)

Table 2-1.Logical Data Structure of the AXSEAL product

2.5 PRODUCT LIFE-CYCLE

The TOE life cycle is described in terms of the four life cycle phases (figure 2-4).

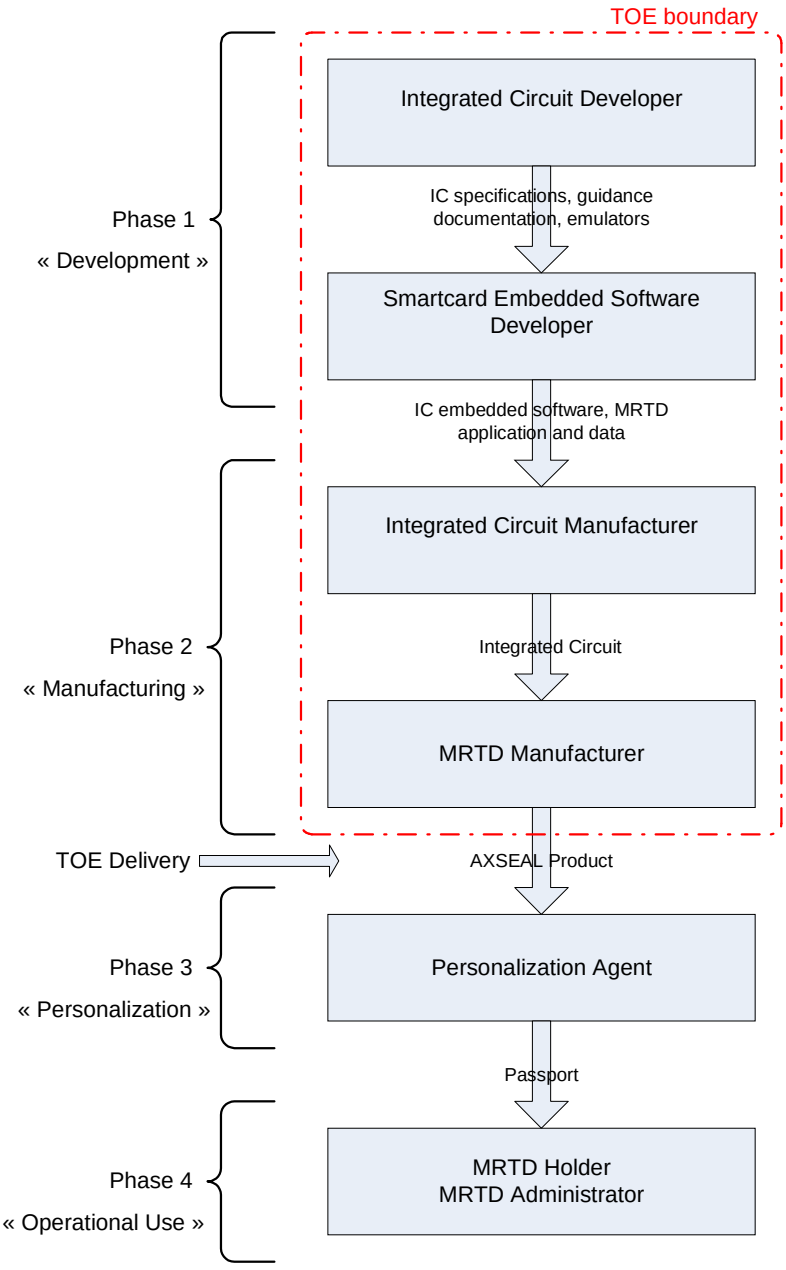


Figure 2-4.Life cycle phases

Phase 1 “Development”:

The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

The Embedded Software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded

Software in the nonvolatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 “Manufacturing”:

In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The MRTD manufacturer:

- add the parts of the IC Embedded Software (NVM ES) in the nonvolatile programmable memories (for instance EEPROM) if necessary,
- creates the MRTD application,
- equips MRTD’s chip with Pre-personalization Data,
- packs the IC with hardware for the contactless interface in the passport book.

Application note [ST]: in the [MRTD-PP], the MRTD Manufacturer could deliver a passport to the Personalization agent. However in this ST, we consider that the MRTD Manufacturer delivers the Axseal product (as described in paragraph 2.4.1) to the Personalization Agent.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 “Personalization of the MRTD”:

The personalization of the MRTD includes:

- the survey of the MRTD holder biographical data,
- the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- the printing of the visual readable data onto the physical MRTD,
- the writing the TOE User Data and TSF Data into the logical MRTD,
- the writing the TSF Data into the logical MRTD and configuration of the TSF if necessary.

The step “writing the TOE User Data” is performed by the Personalization Agent and includes but is not limited to the creation of:

- the digital MRZ data (DG1),
- the digitized portrait (DG2),
- the Document security object (SOD).

The signing of the Document security object by the Document signer [PKI] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application note [MRTD-PP]: The protection profile [MRTD-PP] distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [PKI]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organization, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows for fast authentication protocols appropriate for centralized personalization schemes but relies on stronger security protection in the personalization environment.

Phase 4 “Operational Use”

The TOE is used as MRTD's chip by the traveler and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the Issuing State or Organization and used according to the security policy of the Issuing State but they can never be modified.

Application note [MRTD-PP]: The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify DG16) in the Phase 4 Operational Use. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

Application note [MRTD-PP]: The intention of the PP is to consider at least the phases 1 and 2 as part of the evaluation and therefore define TOE delivery according to CC after phase 2 or later. The personalization process and its environment may depend on specific security needs of an issuing state or organisation. The Security Target shall describe the instantiation of the life cycle defined in this PP relevant for the product evaluation process. It is of importance to define the point of TOE delivery in the life cycle required for the evaluation according to CC requirements ADO_DEL. All development and production steps before TOE delivery have to be part of the evaluation under ACM, ALC and ADO assurance classes as specifically relevant before TOE delivery. All production, generation and installation procedures after TOE delivery up to the operational use (phase 4) have to be considered in the product evaluation process under ADO and AGD assurance classes. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery. Note: In many cases security aspects for phase 3 are defined and controlled by the issuing state or organisation.

Application note [ST]: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. A new actor called MRTD Administrator is introduced for the TOE administration in the phase 4 Operational Use.

Actors	Identification
Integrated Circuit (IC) Developer	Philips
Embedded Software Developer	gemalto
Integrated Circuit (IC) Manufacturer	Philips
MRTD Manufacturer	gemalto
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD Administrator	The Agent acting on behalf of the Issuing State or Organization who is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.

Table 2-2.Identification of the actors

3. TOE SECURITY ENVIRONMENT

3.1 ASSETS

The assets to be protected by the TOE include the User Data on the MRTD's chip.

D.LDS : **Logical MRTD Data**

The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [LDS]. These data are user data of the TOE. The data groups DG1 to DG14 and DG 16 contain personal data of the MRTD holder. The Active Authentication Public Key Info in DG 15 is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRTD.

Application note [ST]:
Assets are exhaustively detailed in the following way:

- data refined in user data and TSF data,
- keys used for product administration and MRTD application.

D. USER_DATA : **User Data**

All user data are protected in integrity and confidentiality.

Data name	Data abbrev.	Location	Function
Machine Readable Zone	MRZ	DG1	Reflects the entire content of the MRZ
Encoded Face	-	DG2	Represents the globally interoperable biometric for machine assisted identity confirmation
Data Groups	DG	DG3 to DG14, DG16	Optional Data (see Table 2-4 for details)
Active Authentication Public Key Info	KPu_{AA}	DG15	Used by Inspection System to check authenticity of the MRTD chip
Security Object Document	SOD	EF.SOD	Contains the signatures used by the inspection system for Passive Authentication of the logical MRTD
Card Production Life Cycle Data	CPLCD	EF.ICC	Traceability data of MRTD chip (see [FSP])
Data Group Presence Map	DGPM	EF.COM	Contains the mandatory header and data group presence information

Table 3-1.User data

Application note [ST]: As the CPLCD identifies uniquely the MRTD's chip, it is possible to trace the MRTD holder (threat T. CHIP_ID), thus access to CPLCD is protected by BAC.

D. TSF_DATA : **TSF Data**

Data name	Data abbrev.	Location	Function
Unique Identification Number	UID	Reserved EEPROM area	Used by the anti-collision mechanism to uniquely identify a chip
Life cycle status	LCS	EEPROM	Data
Send Sequence Counter	SSC	RAM	Counter incremented during secure messaging session
TOE Identification data	-	Founder area, ROM, OTP	Identification of the TOE (chip, hardmask and softmask)

Table 3-2.TSF data

Application note [ST]: As the UID could identify uniquely the MRTD's chip, it is possible to trace the MRTD holder and realizing the threat T. CHIP_ID, thus the fixed value must be replaced by a random value generated each time the chip emitted the UID.

D. KEYS : **Keys**

All the keys are protected in integrity and confidentiality.

Key name	Key abbrev.	Location	Function
AXSEAL personalization and administration keys			
External Keys (1 to 16)	K_{EXT}	EF.key_Ext	Personalization and administration keys
MRTD applicative keys			
Document Basic Access Key	K_{ENC}	EF.key_BAC	Basic Access Control to data of the MRTD application
Document Basic Access Key	K_{MAC}	EF.key_BAC	
Document Basic Access Session Key	KS_{ENC}	RAM	
Document Basic Access Session Key	KS_{MAC}	RAM	
Active Authentication Private Key	KPr_{AA}	$EF.Pr_{AA}$	RSA key used by MRTD chip to generate a signature
Active Authentication Public Key	KPu_{AA}	$EF.Pu_{AA}$	Active Authentication Public key used by the chip for security check

Table 3-3.Keys

An additional asset is the more general following one:

D.MRTD : **Authenticity of the MRTD's chip**

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD's holder is used by the traveler to authenticate himself as possessing a genuine MRTD.

3.2 SUBJECTS

This security target considers the following subjects:

MANUFACTURER :

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

MRTD_HOLDER :

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

TRAVELER :

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

PERSONALIZATION_AGENT :

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

MRTD_ADMINISTRATOR :

The Agent acting on behalf of the Issuing State or Organization who is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 "Operational Use".

INSPECTION_SYSTEM :

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

Not Applicable to this ST: The **Primary Inspection System** (PIS) contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism. The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled.

The **Basic Inspection System** (BIS) contains a terminal for the contactless communication with the MRTD's chip, implements the terminals part of the Basic Access Control Mechanism and gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the printed data in the MRZ or other parts of the passport book providing this information.

The **Extended Inspection System** (EIS) in addition to the Basic Inspection System implements the Active Authentication Mechanism, supports the terminals part of the Extended Access Control Authentication Mechanism and is authorized by the issuing State or Organization to read the optional biometric reference data.

Application note [ST]: The Extended Access Control is outside the scope of this ST. The Extended Inspection System is considered in this ST as it supports the Active Authentication mechanism.

TERMINAL :

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

Application note [ST]: During phase 4 Operational Use, a terminal can be used by an administrator to perform administrative commands like termination of the application.

ATTACKER :

A threat agent trying:

- to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data),
- to read or to manipulate the logical MRTD without authorization,
- to forge a genuine MRTD.

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

Application note [ST]: There are various groups of attackers following different goals. These range from criminals and terrorists to gaming students. Skimming and eavesdropping attacks could be more the fact of criminals trying to capture data in order to make a clone of a passport. Logical and brute force attacks could be realized by game by people aiming to demonstrate their skill. One more specific is the attack against the identification of the holder by skimming TOE identification data. Due to the necessary means to be put in place (several antennas) this attack could be the fact of an organization trying to trace people for criminal, political or commercial goals.

3.3 ASSUMPTIONS

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

A.PERS_AGENT : Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.INSP_SYS : Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

The Basic Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

Application note [ST]: The Extended Inspection System in addition to the Basic Inspection System implements the Active Authentication mechanism.

Application note [ST]: According to the scope of the TOE, the OSP P.PERSONALIZATION and P.PERSONAL_DATA from [MRTD-PP] are now defined as assumptions in the present security target.

Application note [ST]: The following assumptions A.SIGNATURE_PKI, A.AUTH_PKI, A.HOLDER_BEHAV are added to the [MRTD-PP] assumptions.

A.SIGNATURE_PKI: PKI for Passive Authentication

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical MRTD. The issuing State or Organization runs a

Certification Authority (CA) which (i) securely generates, stores and uses the Country Signing CA Key pair, and (ii) manages the MRTD's Active Authentication Key Pairs. The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the MRTDs. The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and organizations.

A.AUTH_PKI: PKI for Active Authentication

The issuing and receiving States or Organisations establish a public key infrastructure for Active Authentication i.e. digital signature creation and verification to prove the chip authenticity. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the DG contents of the logical MRTD (including the public Active Authentication key). The issuing States or Organizations distributes the Active Authentication key pairs of their Country Verifying Certification Authority to their MRTD's chip.

A.HOLDER_BEHAV : Behavior of the MRTD Holder

The MRTD holder uses his passport according to the recommendations guide provided by the issuing State or Organization (non-divulgation of the printed MRZ in operational phase).

3.4 THREATS

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

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

T.CHIP_ID: Identification of MRTD's chip

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

Application note [ST]: To realize this threat the attacker needs several antennas put at dedicated places and also an information system to manage the collected data. This attack can be performed by powerful organization.

T.SKIMMING: **Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.EAVESDROPPING: Eavesdropping to the communication between TOE and inspection system

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

Note: in case of T.SKIMMING the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.EAVESDROPPING the attacker uses the communication of the inspection system.

Application note [ST]: T.SKIMMINGS and T.EAVESDROPPING are the most common contact-less attacks against the user data. For skimming attack the attacker could seat besides the MRTD holder (for example during a plane travel) and performs a combined skimming and brute force attack during several hours.

T.FORGERY: **Forgery of data on MRTD's chip**

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveler into an other MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD in another contactless chip.

T.CLONING: Functional cloning of the TOE

Generally, this threat is derived from specific threats combining unauthorised disclosure, modification or theft of assets. An attacker may utilize design information gained from inspection of the MRTD and/or from eavesdropping attack to fabricate a clone and realize a successful identification on a terminal. The attacker may also realize a skimming attack, with a combined brute force attack extracts completely or partially the data from a genuine MRTD and copies them on another appropriate chip to imitate this genuine MRTD.

Application note [ST]: T.FORGERY and T.CLONING attacks could be performed by criminals with good expertise and equipment level.

T.ABUSE_FUNC: Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational 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 state after delivery to MRTD holder.

Application note [ST]: This threat is also relevant for the misuse or abuse of administrative commands during the phase 4 Operational use. Logical attacks by trying combination of commands or modified commands could be realized with standard equipment by the attacker on the own passport.

T.INFORMATION_LEAKAGE : Information Leakage from MRTD's chip

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).

T.PHYS_TAMPER : Physical Tampering

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

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

T.MALFUNCTION : Malfunction due to Environmental Stress

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

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

Application note [ST]: T.INFORMATION_LEAKAGE, T.PHYS_TAMPER and T.MALFUNCTION are attacks against user data and administrative data. The relevant attacks could be performed with good expertise and equipment level..

3.5 ORGANIZATIONAL SECURITY POLICIES

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

P.MANUFACT: Manufacturing of the MRTD's chip

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.PERSONALIZATION: Personalization of the MRTD by issuing State or Organization only

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

P.PERSONAL_DATA : Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitized portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [PKI].

Application note [MRTD-PP]: The organizational security policy P.PERSONAL_DATA is drawn from the ICAO Technical Report [PKI]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1 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 : Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups DG1 to DG16, the Document security object according to LDS [LDS] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG16 and the TSF data can be written only once and can not be changed after personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups DG 3 to DG16 are added. Only the Personalization Agent shall be allowed to enable or to disable the TSF Basic Access Control.

Application note [MRTD-PP]: The OT.AC_PERS implies that:

- the data of the LDS groups written during personalization for MRTD holder (at least DG1 and DG2) can not be changed by write access after personalization,
- the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordantly.

OT.DATA_INT : Integrity of personal data

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. If the TOE is configured for the use with Basic Inspection Terminals only the TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT.DATA_CONF : Confidentiality of personal data

If the TOE is configured for the use with Basic Inspection Systems the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by (i) as Personalization Agent or as (ii) Basic Inspection System. The Basic Inspection System shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Application note [MRTD-PP]: The traveler grants the authorization for reading the personal data in DG1 to DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.DATA_CONF requires the TOE to ensure the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent.

Any attack based on decision of the ICAO Technical Report [PKI] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.DATA_CONF.

OT.IDENTIFICATION : Identification and Authentication of the TOE

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. If the TOE is configured for use with Basic Inspection Terminals only in Phase 4 “Operational Use” the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note [MRTD-PP]: The TOE security objective OT.IDENTIFICATION addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.IDENTIFICATION addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.MATERIAL. In the Phase 4 “Operational Use” the TOE is identified by the passport number as part of the printed and digital MRZ. If the TOE allows a Primary Inspection System (i.e. every terminal) to read these data every terminal may identify the TOE. If the TOE is configured to allow a Basic Inspection System only to read these data the OT.IDENTIFICATION forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

OT.CHIP_AUTH_PROOF: Proof of MRTD’S chip authenticity

The TOE must support the Extended Inspection Systems to verify the authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [PKI]. The authenticity proof provided by MRTD’s chip shall be protected against attacks with low attack potential.

Application note [ST]: The OT.CHIP_AUTH_PROOF implies the MRTD’s chip to have (i) a unique identity as given by the MRTD’s Document number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD’s chip i.e. a certificate for the Active Authentication Public Key that fit to the Active Authentication Private Key of the MRTD’s chip. This certificate is provided by (i) the Active Authentication Public Key (EF.DG15) in the LDS and (ii) the hash value of the Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.PROT_ABUSE_FUNC : Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order:

- to disclose critical User Data,
- to manipulate critical User Data of the Smartcard Embedded Software,
- to manipulate Soft-coded Smartcard Embedded Software,
- to bypass, deactivate, change or explore security features or functions of the TOE.

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

The following TOE security objectives address the protection provided by the MRTD’s chip independent on the TOE environment.

Application note [ST]: The executable code (called NVM ES in this document for Non Volatile Memory Embedded Software) could be loaded to rectify potential problems in the AXSEAL V2CC ES and/or to add functionalities. After loading, a lock mechanism forbids any modification of the NVM ES.

OT.PROT_INF_LEAK : Protection against Information Leakage

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

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

Application note [MRTD-PP]: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.PROT_PHYS_TAMPER : Protection against Physical Tampering

The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the MRTD'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),
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security features, as well as,
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

Application note [MRTD-PP]: In order to meet the security objectives OT.PROT_PHYS_TAMPER the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.ASSURANCE.

OT.PROT_MALFUNCTION : Protection against Malfunctions

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.

Application note [MRTD-PP]: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT. PROT_PHYS_TAMPER) provided that detailed knowledge about the TOE´s internals.

OT.ADMINISTRATION : Availability of administrative commands in operational use

The TOE must provide secure administrative commands to the TOE administrator in phase 4 Operational use. The TOE must prevent the use of these commands from unauthorized users. These administrative actions involve but are not limited to: reading of the CPCLD, invalidation of the application DF. They are performed by means of administration terminals.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Security Objectives for the Development and Manufacturing Environment

OD.ASSURANCE: **Assurance Security Measures in Development and Manufacturing Environment**

The developer and manufacturer ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing

of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with low attack potential and against direct attacks with high attack potential against security function that uses probabilistic or permutational mechanisms.

OD.MATERIAL : Control over MRTD Material

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialize, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.2.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.PERSONALIZATION: Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographic data for the MRTD, (ii) enrol the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object). The Personalization Agents enable or disable the Basic Access Control function of the TOE according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled the Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip.

OE.PASS_AUTH_SIGN : Authentication of logical MRTD by Signature

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

OE.AUTH_KEY_MRTD: MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

OE.ADMINISTRATION : Administration of logical MRTD

The issuing State or Organization must ensure that the MRTD administrator acting on the behalf of the issuing State or Organization establish the correct identity of the holder and update the MRTD with the defined physical and logical security measures. According to the decision of the issuing State or Organization the MRTD administrator can for example terminate the application or execute any administrative commands provided by the TOE.

Receiving State or organization

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

OE.EXAM_MRTD : Examination of the MRTD passport book

The inspection system of the Receiving State must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD.

Application note [ST]: Additionally the Extended Inspection System performs the Active Authentication mechanism to verify the Authenticity of the presented MRTD's chip.

OE.PASSIVE_AUTH_VERIF: Verification by Passive Authentication

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

OE.PROT_LOGICAL_MRTD : Protection of data of the logical MRTD

The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.

Application note [ST]: The original security objective of the TOE environment OE.SECURE_HANDLING from the PP is not applicable as the mode with disabled BAC is out of the ST scope. The following definition is specified for this objective.

MRTD Holder

OE.SECURE_HANDLING : Secure handling of the MRTD by MRTD holder

The holder may prevent attempts to disclose the logical MRTD by following recommendations for the protection of the MRZ against unauthorized people. An attacker knowing the MRZ or a part of it have better chance to perform a successful skimming or eavesdropping attack.

5. IT SECURITY REQUIREMENTS

5.1 EXTENDED COMPONENTS DEFINITION

This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [SSVGPP], other components are defined in the protection profile [MRTD-PP].

5.1.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

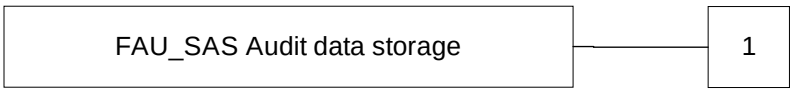
The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component leveling



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
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.

5.1.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here.

This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

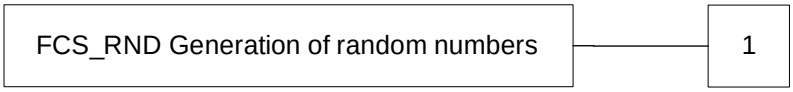
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1

	There are no management activities foreseen.
Audit:	FCS_RND.1
	There are no actions defined to be auditable.

FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].
Dependencies:	No dependencies.

5.1.3 Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE an additional family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of a claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application note [MRTD-PP]: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter Explicitly stated IT security requirements (APE_SRE)) form a TOE point of view. Note: the protection profile uses this explicit stated SFR for the personalization terminal in the IT environment only. Therefore the word "TSF" is substituted by the word "Personalization terminal".

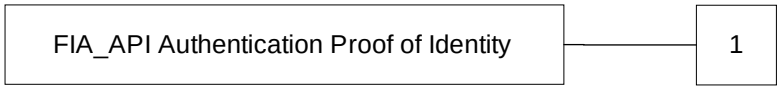
Application note [ST]: This security target uses this SFR for the TOE for the Active Authentication and the Chip Authentication mechanisms.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:



FIA_API	Authentication Proof of Identity
FIA_API.1	Authentication Proof of Identity.
Management:	FIA_API.1
	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	There are no actions defined to be auditable.

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
FIA_API.1.1	The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule].
Dependencies:	No dependencies.

5.1.4 Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

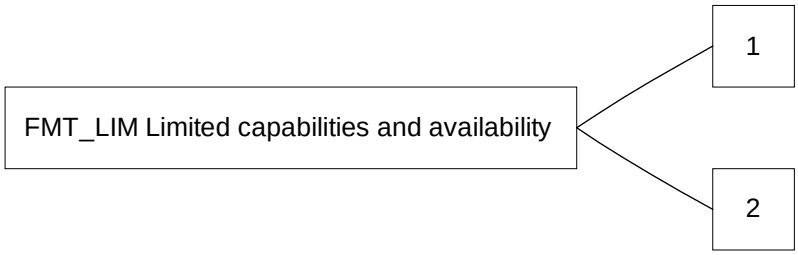
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:



FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the

mana
gement of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
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 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
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 Limited capabilities.

Application note [MRTD-PP]: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced or conversely the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

5.1.5 Definition of the Family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE.

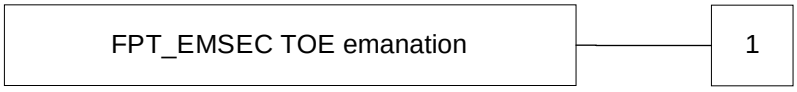
The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC].

The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions defined to be auditable.

FPT EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
FPT_EMSEC.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_EMSEC.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 other components.

5.2 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

5.2.1 Class FAU Security Audit (FAU)

The TOE shall meet the requirement “Security Audit (FAU_ARP.1)” as specified below (Common Criteria Part 2).

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **[assignment: list of the least disruptive actions]** upon detection of a potential security violation.

Refinement:

Assignment: Disruptive actions taken upon detection of following potential security violation	
Disruptive actions	Potential security violation
Reset	Voltage supply out of range or specifications
Reset	Signals out of range or specifications
Reset	Temperature out of range
Reset or exception then reset	Exposure to light
Exception then reset	Corrupted integrity of PC, SP/SPE, PSWH
Exception then reset	Corrupted integrity of Triple-DES co-processor
Exception then reset	Corrupted integrity of FameXE
Exception then reset	Illegal instructions
Exception then reset	Unauthorized system calls
Exception then reset	Memory access violation
Exception then reset	Access collisions
Exception then reset	Stack overflow
Error status word	EEPROM writing error
Error status word	Corrupted integrity of user data
Chip is mute	Corrupted integrity of TSF data
Chip is mute	Wrong verification of TDES execution
Chip is mute	Wrong verification of RSA execution
Chip is mute	Software detection of abnormal execution

Table 5-1.Security Audit

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (Common Criteria Part 2 extended).

FAU_SAS.1 Audit storage

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

Application note [MRTD-PP]: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_DEL ensure that the audit records will be used to fulfill the security objective OD.ASSURANCE.

5.2.2 Class Cryptographic Support (FCS)

The Table below provides an overview on the cryptographic mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Symmetric Authentication Mechanism for Personalization	FCS_COP.1.1/TDES_MRT FCS_RND.1/MRTD	FCS_COP.1.1/ENC_BT	Triple-DES with 112 bits keys
Symmetric Authentication Mechanism for Administration	FCS_COP.1.1/TDES_MRT FCS_RND.1/MRTD	FCS_COP.1.1/ENC_BT	Triple-DES with 112 bits keys
Basic Access Control Authentication Mechanism	FCS_CKM.1.1/BAC_MRTD FCS_CKM.4.1/MRTD FCS_COP.1.1/SHA_MRTD FCS_COP.1.1/TDES_MRT FCS_COP.1.1/MAC_MRT FCS_RND.1/MRTD	FCS_CKM.1.1/BAC_BT FCS_CKM.4.1/BT FCS_COP.1.1/SHA_BT FCS_COP.1.1/ENC_BT FCS_COP.1.1/MAC_BT FCS_RND.1/BT	Triple-DES, 112 bits keys, Retail-MAC, 112 bits keys
Active Authentication Mechanism	FCS_COP.1.1/RSA_AA	FCS_RND.1/BT FCS_COP.1.1/ET_AA	RSA Signature, 1024 bits key

Table 5-2.Cryptographic support

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/BAC_MRTD Cryptographic key generation – Generation of Document Basic Access Keys by the TOE

FCS_CKM.1.1/BAC_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Control Key Derivation Algorithm** and specified cryptographic key sizes **112 bit** that meet the following: **[PKI], Annex E 7**.

Application note [MRTD-PP]: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [PKI], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [PKI], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

FCS_CKM.4/MRTD Cryptographic key destruction - MRTD

FCS_CKM.4.1/MRTD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Refinement:

Key	Assignment: Cryptographic key destruction method	Assignment: List of standards
Document Basic Access Session Keys	Secure erasing of the value	None

Table 5-3.Cryptographic key destruction

Application note [MRTD-PP]: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA_MRTD Cryptographic operation - Hash for Key Derivation by MRTD

FCS_COP.1.1/SHA_MRTD The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS180-2**.

Application note [MRTD-PP]: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4/MRTD) according to [PKI].

FCS_COP.1/TDES_MRTD Cryptographic operation –Encryption / Decryption Triple DES

FCS_COP.1.1/TDES_MRTD The TSF shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3 [14] and [PKI]; Annex E 15**.

Application note [MRTD-PP]: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FIA_UAU.4/BAC_BT. Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.

Application note [ST]: The Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as MRTD Administrator by means of the symmetric authentication mechanism.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

FCS_COP.1.1/MAC_MRTD The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bits** that meet the following: **ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).**

Application note [MRTD-PP]: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/MRTD.

FCS_COP.1/RSA_AA Cryptographic operation – RSA Signature Computation - Active Authentication

FCS_COP.1.1/RSA_AA The TSF shall perform **Signature computation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024 bits** that meet the following: **ISO9796-2**.

Application note [ST]:The minimum key size recommended in [PKI] is 1024 bits.

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1/MRTD Quality metric for random numbers

FCS_RND.1.1/MRTD The TSF shall provide a mechanism to generate random numbers that meet **the requirement to provide an entropy of at least 7.976 bit in each byte.**

Application note [MRTD-PP]: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4/MRTD.

5.2.3 Class Identification and Authentication (FIA)

The Table below provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Symmetric Authentication Mechanism for Personalization	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bits keys
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/BT FIA_UAU.6/BT	Triple-DES, 112 bits keys, Retail-MAC, 112 bits keys
Active Authentication Mechanism	FIA_API.1/MRTD	FIA_UAU.4/ET	RSA Signature, 1024 bits key
Symmetric Authentication Mechanism for Administration	FIA_UAU.4/MRTD	FIA_API.1/AT	Triple-DES with 112 bits keys

Table 5-4.Identification and authentication

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API)” as specified below (Common Criteria Part 2 extended).

FIA_API.1/MRTD Authentication Proof of Identity - TOE Authentication

FIA_API.1.1/MRTD The TSF shall provide an **[assignment: authentication mechanism]** to prove the identity of the **[assignment: authorised user or role]**.

Refinement:

Assignment: authentication mechanism	Assignment: authorised user or role
Active Authentication Mechanism based on RSA signature	MRTD chip

Table 5-5. Authentication Proof of Identity

This SFR requires the TOE to implement the Active Authentication Mechanism specified in [PKI]. The terminal verifies by means of signature verification whether the MRTD’s chip was able or not to sign properly the generated random using its Active Authentication Private Key.

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (Common Criteria Part 2).

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[assignment: list of TSF-mediated actions]** 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.

Refinement:

Assignment: list of TSF-mediated actions	Refinement: Command
to read the Initialization Data in Phase 2 “Manufacturing”	READ DATA
to read the ATS in Phase 3 “Personalization of the MRTD”	RATS sent by the Personalization Terminal
to read the ATS in Phase 4 “Operational Use”	RATS sent by the Basic Inspection System

Table 5-6. Timing of identification

Application note [MRTD-PP]: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”.

The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys.

If the TOE is configured for use with Basic Inspection Systems only the Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System according to the SFR FIA_UAU.4/BT.

Application note [MRTD-PP]: In the operation phase the MRTD must not allow anybody to read the ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.CHIP_ID). Note that the terminal and the MRTD’s chip use an identifier for the communication channel to allow the terminal for communication with more then one RFID. If this identifier is randomly selected it will not violate the OT.IDENTIFICATION. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.CHIP_ID.

Application note [ST]: The ATS is only relevant for type A protocol chip and in this case it is sent in all phases.

The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (Common Criteria Part 2).

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **[assignment: list of TSF mediated actions]** 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.

Refinement:

Assignment: list of TSF-mediated actions	Refinement: Command
to read the Initialization Data in Phase 2 “Manufacturing”	READ DATA
to read the ATS in Phase 3 “Personalization of the MRTD”	RATS sent by the Personalization Terminal
to read the ATS in Phase 4 “Operational Use”	RATS sent by the Basic Inspection System

Table 5-7.Timing of authentication

Application note [ST]: The Basic Inspection System, the Personalization Agent, the Extended Inspection System and the Administration Terminal authenticate themselves.

Application note [ST]: The ATS is only relevant for type A protocol chip and in this case it is sent in all phases.

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

FIA_UAU.4.1/MRTD The TSF shall prevent reuse of authentication data related to **[assignment: identified authentication mechanism(s)]**.

Refinement:

Assignment: Identified authentication mechanisms
Authentication Mechanisms based on Triple-DES
Basic Access Control Authentication Mechanism

Table 5-8.Single-use authentication mechanisms

Application note [MRTD-PP]: All listed authentication mechanisms uses a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: the Basic Access Control Authentication Mechanism uses RND.ICC [PKI], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.

Application note [MRTD-PP]: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [PKI]. In the first step the terminal authenticates themselves to the MRTD’s chip and the MRTD’s chip authenticates to the terminal in the second step. In this second step the MRTD’s chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD’s chip with some probability depending on the entropy of the Document Basic Access Control Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfill the security objective OT.IDENTIFICATION and to prevent T.CHIP_ID.

Application note [ST]: The Authentication Mechanism based on Triple-DES is used for Personalization Agent authentication by means of the Personalization Terminal and for MRTD Administrator Authentication by means of the Administration Terminal.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **[assignment: list of multiple authentication mechanisms]** to support user authentication.

Refinement:

Assignment: list of multiple authentication mechanisms
Symmetric Authentication Mechanism based on Triple-DES
Basic Access Control Authentication Mechanism

Table 5-9.Multiple authentication mechanisms

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **[assignment: rules describing how the multiple authentication mechanisms provide authentication]**.

Refinement:

Assignment: rules describing how the multiple authentication mechanisms provide authentication
the TOE accepts the authentication attempt as Personalization Agent by means of the Symmetric Authentication Mechanism with the Personalization Agent Key.
the TOE accepts the authentication attempt as Basic Inspection System or as Extended Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys
the TOE accepts the authentication attempt as MRTD Administrator by means of the Symmetric Authentication Mechanism with the Administrative Keys.

Table 5-10.Multiple authentication mechanisms

Application note [ST]: The Authentication Mechanism based on Triple-DES is the only mean of authentication usable by the Personalization Agent.

Application note [MRTD-PP]: Depending on the authentication methods used the Personalization Agent holds (i) a pair of a Triple-DES encryption key and a retail-MAC key for the Basic Access Control Mechanism specified in [PKI], or (ii) a Triple-DES key for the Symmetric Authentication Mechanism. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Note: the successful authenticated Personalization Agent may disable the Basic Access Control Mechanism.

The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below (Common Criteria Part 2).

FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE

FIA_UAU.6.1/MRTD The TSF shall re-authenticate the user under the conditions **[assignment: list of conditions under which re-authentication is required]**.

Refinement:

Assignment: Conditions under which re-authentication is required
each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism

Table 5-11.Re-authenticating

Application note [MRTD-PP]: The Basic Access Control Mechanism specified in [PKI] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticate the user for each received command and accept only those commands received from the initially authenticated by means of BAC user.

The TOE shall meet the requirement “Timing of identification (FIA_AFL.1)” as specified below (Common Criteria Part 2).

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **a positive integer number or an administrator configurable positive integer within a range of acceptable values (see table below)** unsuccessful authentication attempts occur related to **specified authentication events (see table below).**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions (see table below)].**.

Refinement:

Assignment: Number	Assignment: Specified Authentication events	Assignment: Actions
3	Unsuccessful External Authenticate Command with Personalization Agent Keys	Personalization Agent Keys blocked
1	Unsuccessful Basic Access Control Authentication	Random generated by the card for the mutual authentication is made unavailable, a new one must be generated for another mutual authentication attempt
1	Unsuccessful MAC verification after Basic Access Control Authentication	Basic Access Session keys unavailable
3	Unsuccessful External Authenticate Command with EFkeyext key used for the prepersonalization	Key blocked

Table 5-12. Basic authentication failure

Note: EFkeyext administrative key used for the TERMINATE and GET DATA commands has no counter.

The TOE shall meet the requirement “Timing of identification (FIA_ATD.1)” as specified below (Common Criteria Part 2).

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: list of security attributes]**.

Refinement:

User	Assignment: Security attributes
Personalization Agent	Personalization key authentication status
MRTD Holder	BAC authentication status Terminal Authentication status MAC verification status
MRTD Administrator	External key authentication status

Table 5-13. User attribute definition

5.2.4 Class User Data Protection (FDP)

The TOE shall meet the requirement “Subset access control (FDP _ACC.1)” as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

Following SFR is not applicable to this ST and is deleted from the original PP: FDP_ACC.1/PRIM

FDP_ACC.1/BASIC Subset access control – Basic Access control

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

FDP_ACC.1/AUTH Subset access control – External Authentication Access control

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

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 address different SFP.

Following SFR is not applicable to this ST and is deleted from the original PP: FDP_ACF.1/PRIM

FDP_ACF.1/BASIC Security attribute based access control – Basic Access Control

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

1. **Subjects:**

   - **Basic Inspection System,**
   - **Extended Inspection System,**
   - **Administration terminal,**
   - **Terminal.**

2. **Objects:**

   - **data in the data groups DG1 to DG16 of the logical MRTD,**
   - **data in EF.COM,**
   - **data in EF.SOD,**
   - **data in EF.ICC,**
   - **data in EF.DIR.**

3. **Security attributes:**

   - **authentication status of terminals.**

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

1. **the successfully authenticated Basic Inspection System is allowed to read data of the data groups DG1 to DG16 of the logical MRTD, EF.COM, EF.SOD, EF.ICC.**

2. **the successfully authenticated Extended Inspection System is allowed to read data of the data groups DG1 to DG16 of the logical MRTD, EF.COM, EF.SOD, EF.ICC.**

3. **the successfully authenticated Administration terminal is allowed to read data of the data groups DG1 to DG16 of the logical MRTD, EF.COM, EF.SOD, EF.ICC.**

FDP_ACF.1.3/BASIC The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **Basic Inspection System, Extended Inspection System and Administration terminal are allowed to read data in EF.DIR**.

FDP_ACF.1.4/BASIC The TSF shall explicitly deny access of subjects to objects based on the rule: **the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD, EF.COM, EF.SOD, EF.ICC, EF.DIR.**

Application note [MRTD-PP]: FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

FDP_ACF.1/AUTH Security attribute based access control – External Authentication Access Control

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

1. **Subjects:**
   - **Personalization Agent,**
   - **Terminals.**
2. **Objects:**
   - **data in the data groups DG1 to DG16 of the logical MRTD,**
   - **data in EF.COM,**
   - **data in EF.SOD,**
   - **data in EF.ICC,**
   - **data in EF.DIR.**
3. **Security attributes**
   - **authentication status of terminals.**

FDP_ACF.1.2/AUTH 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 data of files: EF.DG1 to EF.DG16 of the logical MRTD, EF.COM, EF.SOD, EF.ICC, EF.DIR.**

FDP_ACF.1.3/AUTH The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **Personalization Agent is allowed to read data in EF.DIR**.

FDP_ACF.1.4/AUTH The TSF shall explicitly deny access of subjects to objects based on the rule: **none**.

The TOE shall meet the requirement “Stored data integrity monitoring and action (FDP_RIP.1)” as specified below (Common Criteria Part 2).

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **[assignment: list of objects]**.

Refinement:

Selection	Assignment: List of objects
Deallocation of the resource from	Session Keys

Table 5-14. Subset residual information protection

The TOE shall meet the requirement “Stored data integrity monitoring and action (FDP_SDI.2)” as specified below (Common Criteria Part 2).

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for **[assignment: integrity errors]** on all objects, based on the following attributes: **[assignment: user data attributes]**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **[assignment: action to be taken]**.

Refinement:

Assignment: Integrity errors on following objects	Assignment: User data attributes	Assignment: Action to be taken
External Keys	Checksum	Error status word is emitted, command is aborted
Document Basic Access Keys	Checksum	Error status word is emitted, command is aborted
Active Authentication Key Pair	Checksum	Error status word is emitted, generation of RSA signature is aborted
DG1 to DG16 data	Checksum	Error status word is emitted, data cannot be updated anymore nor used
EF.SOD data	Checksum	Error status word is emitted, data cannot be used anymore
EF.COM	Checksum	Error status word is emitted, data cannot be used anymore
EF.ICC	Checksum	Error status word is emitted, data cannot be used anymore
EF.DIR	Checksum	Error status word is emitted, data cannot be used anymore

Table 5-15. Stored data integrity monitoring and action

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1/MRTD Basic data exchange confidentiality – MRTD

FDP_UCT.1.1/MRTD The TSF shall enforce the **Basic Access Control SFP and External Authentication Access Control SFP** to be able to **transmit and receive** objects in a manner protected from unauthorized disclosure.

The TOE shall meet the requirement "Basic data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1/MRTD Data exchange integrity – MRTD

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

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

5.2.5 Class Security Management (FMT)

The TOE shall meet the requirement "Management of functions in TSF (FMT_MOF.1)" as specified below (Common Criteria Part 2).

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: determine the behaviour of, disable, enable and modify the behaviour of]** the functions **[assignment: list of functions]** to **[assignment: the unauthorized identified roles]**.

Refinement:

Selection: Actions	Assignment: List of functions	Assignment: Authorized identified roles
Modify the behaviour of	TSF External Authenticate Access Control	Personalization Agent
Enable	TSF Basic Access Control	Personalization Agent
Disable	Access to MRTD application (Terminate command)	MRTD Administrator

Table 5-16. Management of security functions behaviour

Application note [ST]: the TOE enforces the Basic Access Control SFP according to FDP_ACC.1/BASIC and FDP _ACF.1/BASIC. In this case the reading of the logical MRTD requires successful authentication as Basic Inspection System, Extended Inspection System, Administration Terminal.

Application note [MRTD-PP]: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

The TOE shall meet the requirement “Specification of Management Functions (FMT_MSA.1)” as specified below (Common Criteria Part 2).

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **access control SFP** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **[assignment: list of security attributes]** to **[assignment: the authorised identified roles]**.

Refinement:

Selection / Assignment: Other operations	Assignment: List of security attributes	Assignment: Authorized identified roles
Enable	NVM ES loading	MRTD Manufacturer
Modify	Life cycle status	MRTD Manufacturer
Modify	Life cycle status	Personalization agent
Modify	Life cycle status	MRTD Administrator

Table 5-17. Management of security attributes

The TOE shall meet the requirement “Specification of Management Functions (FMT_MSA.2)” as specified below (Common Criteria Part 2).

FMT_MSA.2/LIFE_CYCLE Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Application note [ST]: Only defined values are accepted for the life cycle status.

The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (Common Criteria Part 2).

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[assignment: security management functions provided by the TSF (see table below)]**.

Refinement:

Security management functions	Refinement
Initialization	CPLCD loading NVM ES loading Personalization Agent key update Creation of the application DF Life cycle status update
Personalization	CPLCD loading Personalization LDS Keys update Life cycle status update
Administration	Termination of the application (Life cycle status update) Get data (reading of TOE identification data)

Table 5-18. Specification of management functions

Application note [ST]: Security management functions are defined for the administration of the TOE in phase 4 “Operational use”.

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (Common Criteria Part 2).

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: the authorised identified roles]**.

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

Refinement:

Assignment: Authorized identified roles
Manufacturer
Personalization Agent
Basic Inspection System
Extended Inspection System
MRTD Administrator

Table 5-19. Security roles

Application note [MRTD-PP]: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

Application note [ST]: The Extended Inspection System and MRTD Administrator roles are added.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 extended).

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**

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

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

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**

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

Application note [MRTD-PP]: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data

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

Application note [MRTD-PP]: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Authentication Key.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **disable read access for users to** the **Initialization Data and pre-personalization Data (TOE identification data)** to **the Personalization Agent**.

Application note [MRTD-PP]: According to P.MANUFACT the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2.

The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

Application note [ST]: Access to the execution of GET DATA command (reading of TOE identification data) is submitted to a successful administrator authentication. The key used for this authentication is written either by the pre-personalizer or the personalization agent. The CPLC data (unique identification of the chip for traceability) are user data located in EF.ICC with read access submitted to BAC authentication at the end of personalization.

FMT_MTD.1 /INI_READ Management of TSF data – Reading of Initialization Data and Pre-personalization Data

FMT_MTD.1.1/INI_READ The TSF shall restrict the ability to **read** the **Initialization Data and Pre-personalization Data (TOE identification data)** to **the MRTD Administrator**.

Application note [ST]: Reading of initialization data and pre-personalization data (TOE identification data) is submitted to a successful Administrator authentication with the relevant External Key.

FMT_MTD.1 /KEY_WRITE Management of TSF data – Key Write

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys (file EF.key_BAC), the Active Authentication key pair (files EF.Pr_{AA}, EF.Pu_{AA}), the External keys (file EF.key_Ext)** to the **Personalization Agent**.

FMT_MTD.1 /KEY_READ Management of TSF data – Key Read

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the **Document Basic Access Keys (file EF.key_BAC), the Active Authentication Private key (file EF.Pr_{AA}), the External keys (file EF.key_Ext)** to **none**.

Application note [MRTD-PP]: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys, Active Authentication key pair, External keys.

5.2.6 Class Protection of the Security Functions (FPT)

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below (Common Criteria Part 2 extended).

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.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]**.

Refinement:

Assignment: Types of emissions	Assignment: Specified limits	Assignment: List of types of TSF data	Assignment: List of types of user data
Electromagnetic and current emissions	Intelligible threshold	Personalization Agent Authentication Key	DG1 to DG16
	Intelligible threshold	External Keys (Administrative keys)	EF.ICC
	Intelligible threshold	Document Basic Access keys	EF.SOD
	Intelligible threshold	Active Authentication Private Key	EF.COM
	Intelligible threshold	TOE identification data	-

Table 5-20 TOE Emanation

FPT_EMSEC.1.2 The TSF shall ensure **any unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **[assignment: list of types of TSF data]** and **[assignment: list of types of user data]**.

Refinement:

Assignment: List of types of TSF data	Assignment: List of types of user data
Personalization Agent Authentication Key	DG1 to DG16

Assignment: List of types of TSF data	Assignment: List of types of user data
External Keys (Administrative keys)	EF.ICC
Document Basic Access keys	EF.SOD
Active Authentication Private Key	EF.COM
TOE identification data	-

Table 5-21 TOE Emanation: smart card circuit contacts

Application note [MRTD-PP]: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) additional contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

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: **[assignment: list of types of failures in the TSF]**.

Refinement:

Assignment: Types of failures in the TSF
exposure to operating conditions where therefore a malfunction could occur
failure detected by TSF according to FPT_TST.1
Inconsistent TSF data
Interruption/failure during EEPROM write or update operation

Table 5-22 Failure with preservation of secure state

The TOE shall meet the requirement "TSF testing (FPT _TST.1)" as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions][assignment: conditions under which self test should occur]** to demonstrate the correct operation of the TSF.

Refinement:

Selection and Assignment: Conditions under which self test should occur	Refinement: Description of the self test
At UID generation	Test of the random generator
At reception of the first command	Integrity Check of the NVM ES Statistical test of the random generator Integrity check of the anti-tearing area
Before execution of any command	Integrity check of the life cycle status Test of the random generator Integrity check of the right flags
Before cryptographic computation	Test of the random generator
After cryptographic computation	For DES computation: the last DES computation is checked For RSA computation: a signature verification performed Test of the random generator
Before any use or update of TSF data	Integrity check

Table 5-23 TSF testing

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 stored TSF executable code.

Application note [MRTD-PP]: If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Manufacturer in the Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[assignment: physical tampering scenarios]** to the **[assignment: list of TSF devices/elements]** by responding automatically such that the TSP is not violated.

Refinement:

Application note [ST]: Related component FPT_PHP.3 information is provided in document [STPhilips]. All the potential security violations managed by the component are included in the table below. Implemented software mechanisms provide protection against other security violations.

Assignment: Physical tampering scenarios	Assignment: List of TSF devices / elements
Physical manipulation and physical probing	Sensors
The external voltage supply is put out of range	Supply voltage sensors
The external clock signal is put out of range	Frequency sensors
The temperature is put out of range	Temperature sensors
Chip is exposed to light	Light sensors
Attempt to corrupt integrity of pointers	Redundant logic of PC, SP/SPE, PSWH
Attempts to corrupt the TDES computation	Triple-DES fault check
Attempts to corrupt the RSA computation	FameXE fault check
Attempts to run illegal instructions	Exception handling
Attempts to execute unauthorized system calls	Exception handling
Attempts to gain access to sensitive memory area	Exception handling
Attack which generates access collisions	Exception handling
Attempts to overflow the stack	Exception handling
Attempts to corrupt sensitive data writing	EEPROM writing check
Attempts to corrupt integrity of user data	Integrity check of user data
Attempts to corrupt integrity of TSF data (file headers, security attributes…)	Integrity check of TSF data
Attempts to corrupt the random number generator	Random number generator test
Attempts to corrupt the TDES computation	TDES verification
Attempts to corrupt the RSA computation	RSA verification
Attempts to disrupt the code execution	Software execution tracers

Table 5-24 Resistance to physical attack

Application note [MRTD-PP]: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

The TOE shall meet the requirement “Non-bypassability of the TSP (FPT_RVM.1)” as specified below (Common Criteria Part 2).

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by un-trusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application note [MRTD-PP]: The parts of the TOE which support the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” should be protected from interference of the other security enforcing parts of the MRTD’s chip Embedded Software.

5.3 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components: ADV_IMP.2 and ALC_DVS.2.

The minimum strength of function is SOF-high.

Application note [MRTD-PP]: The high minimum strength of function covers but is limited to the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or permutational mechanisms are involved, e.g. due to challenges generated by the TOE and sent to the terminal or probabilistic self tests.

This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

5.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

This section describes the security functional requirements for the IT environment using the CC part 2 components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in ***italic/bold***.

5.4.1 Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (DG1 to DG16) by means of the Document Security Object. The Technical Report [PKI] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the Issuing State or Organization shall meet the requirement “Basic data authentication (FDP_DAU.1)” as specified below (Common Criteria Part 2).

FDP_DAU.1 /DS Basic data authentication – Passive Authentication

FDP_DAU.1.1/DS The ***Document Signer*** shall provide a capability to generate evidence that can be used as a guarantee of the validity of **logical data structure of the MRTD (DG1 to DG16) and the Document Security Object**.

FDP_DAU.1.2/DS The ***Document Signer*** shall provide **Inspection Systems of Receiving States or Organization** with the ability to verify evidence of the validity of the indicated information.

5.4.2 Basic Inspection Systems

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called “Basic Terminals” (BT) in this section.

The Basic Terminal shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal

FCS_CKM.1.1/BAC_BT The ***Basic Terminal*** shall generate cryptographic keys in BAC_BT accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [PKI], Annex E 74.

Application note [MRTD-PP]: The terminals derive the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [PKI], 3.2.2 and Annex E.1, use them to generate the Document Basic Access Keys. The Personalization Agent downloads these keys to the MRTD's chip as TSF data for FIA_UAU.4/MRTD.

The Extended terminal shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

FCS_CKM.4/BT Cryptographic key destruction - BT

FCS_CKM.4.1/BT The ***Basic Terminal*** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **secure erase of the key value** that meets the following: **none**.

Application note [MRTD-PP]: The BIS shall destroy the Document Basic Access Keys of the MRTD and the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after inspection of the MRTD.

The Basic Terminal shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the Basic Terminal.

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

FCS_COP.1.1/SHA_BT The ***Basic Terminal*** shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS180-2**.

Application note [MRTD-PP]: This SFR requires the terminal to implement the hash function SHA-1 for the cryptographic primitive to generate the Document Basic Access Keys according to FCS_CKM.1/BAC_BT.

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

FCS_COP.1.1/ENC_BT The ***Basic Terminal*** shall perform **secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)**.

Application note [MRTD-PP]: This SFR requires the Basic Terminal to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The key is agreed between the TOE and the terminal during the execution of the Basic Access Control Authentication Mechanism. The key size of 112 bit is chosen to resist attacks with high attack potential.

FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

FCS_COP.1.1/MAC_BT The ***Basic Terminal*** shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2).**

Application note [MRTD-PP]: This SFR requires the terminal to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed or defined as the key for secure messaging encryption. The key size of 112 bit is chosen to resist attacks with high attack potential.

The Basic Terminal shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1/BT Quality metric for random numbers by Basic Terminal

FCS_RND.1.1/BT The ***Basic Terminal*** shall provide a mechanism to generate random numbers that meets **the requirement to provide an entropy of at least 7.976 bit in each byte**.

Application note [MRTD-PP]: This SFR requires the terminal to generate random numbers used in the authentication protocols as required by FCS_CKM.1/BAC_BT and FIA_UAU.4 The quality metric shall be chosen to ensure at least the strength of function Basic Access Control Authentication for the challenges.

The Basic Terminal shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

FIA_UAU.4/BT Single-use authentication mechanisms –Basic Terminal

FIA_UAU.4.1/BT The ***Basic Terminal*** shall prevent reuse of authentication data related to **Basic Access Control Authentication Mechanism**.

Application note [MRTD-PP]: The Basic Access Control Authentication Mechanism [PKI] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD’s chip and of the session keys from a successful run of authentication protocol.

The Basic Terminal shall meet the requirement “Re-authentication (FIA_UAU.6)” as specified below (Common Criteria Part 2).

FIA_UAU.6/BT Re-authentication - Basic Terminal

FIA_UAU.6.1/BT The ***Basic Terminal*** shall re-authenticate the user under the conditions **each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism**.

Application note [MRTD-PP]: The Basic Access Control Mechanism specified in [PKI] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The terminal checks by secure messaging in MAC_ENC mode each MRTD's chip response to a command based on Retail-MAC whether it was sent by the successfully authenticated MRTD's chip. The authentication fails if any response is received with incorrect message authentication code.

Application note [MRTD-PP]: The Basic Access Control SFP of the TOE requires to protect the User Data by access control (cf. FDP_ACC.1/BASIC and FDP_ACF.1/BASIC) and by secure messaging (cf. FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) for the communication between the TOE and the Basic Terminal. This secure messaging requires the Basic Terminal to support the protection of the TOE data by decryption and checking MAC and to protect its own data by secure messaging as well. The SFP of the Basic Terminal drawn from the TOE "Basic Access Control SFP" is named "BT part of Basic Access Control SFP" and the related SFR is described by FDP_UCT.1/BT and FDP_UIT.1/BT corresponding to FDP_UCT.1/MRTD and FDP_UIT.1/MRTD of the communication partner (i.e. the TOE). Note the Basic Terminal does not enforce any named access control policy or information control policy to be defined by FDP_ACC and FDP_ACF or FDP_IFC and FDP_IFF families (respectively). The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The Basic Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UCT.1/BT Basic data exchange confidentiality - Basic Terminal

FDP_UCT.1.1/BT The ***Basic Terminal*** shall enforce the **Basic Access Control SFP** to be able to **transmit and receive** objects in a manner protected from unauthorised disclosure.

The Basic Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1/BT Data exchange integrity - Basic Terminal

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

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

5.4.3 Extended Inspection Terminals

The Extended Inspection System (EIS) is a Basic Inspection System which implements additionally the Active Authentication Mechanism. Therefore it has to fulfill all security requirements of the Basic Inspection System as described above.

The Extended Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Active Authentication Mechanism is the Active Authentication Public Key read form the logical MRTD data group EF.DG15 and verified by Passive Authentication.

The Extended Terminal shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2).

FCS_COP.1/ET_AA Cryptographic operation – RSA signature verification

FCS_COP.1.1/ET_AA The ***Extended Terminal*** shall perform **Signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **up to 2048 bits** that meet the following: **ISO9796-2**.

Application note [ST]:The minimum key size recommended in [PKI] is 1024 bits.

The Extended Terminal shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4/ET Single-use authentication mechanisms –Single-use authentication of the TOE by the Extended Terminal

FIA_UAU.4.1/ET The ***Extended Terminal*** shall prevent reuse of authentication data related to **Active Authentication Mechanism**.

Application note [ST]: The Active Authentication Mechanism [PKI] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD's chip from a successful run of authentication protocol.

5.4.4 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

1. The Basic Access Control Mechanism which may be used by the Personalization Agent with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the personalization terminal may be listened or manipulated (*Not applicable to this ST:* the Axseal product is not intended to be used by the Personalization Agent with the Basic Access Control Mechanism).
2. In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple protocol as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

The Personalization Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended).

FIA_API.1/SYM_PT Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Key

FIA_API.1.1/SYM_PT The ***Personalization Terminal*** shall provide an **Authentication Mechanism based on Triple-DES** to prove the identity of the **Personalization Agent**.

Application note [MRTD-PP]: The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD's chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [ISO] command. In this case the communication may be performed without secure messaging (note that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control Authentication).

5.4.5 Administration Terminals

For the administration the TOE and the Administration Terminal support a simple protocol as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_AT

The Administration Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below (Common Criteria Part 2 extended).

FIA_API.1/SYM_AT Authentication Proof of Identity - Administration Terminal Authentication with Symmetric Key

FIA_API.1.1/SYM_PT The ***Administration Terminal*** shall provide an **Authentication Mechanism based on Triple-DES** to prove the identity of the **MRTD Administrator**.

Application note [ST]: The Symmetric Authentication Mechanism for MRTD Administrators is intended to be used in a high secure environment only. It uses a symmetric cryptographic Administrative Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD's chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [ISO] command. In this case the communication may be performed without secure messaging.

6. TOE SUMMARY SPECIFICATION

6.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the Axseal V2CC embedded software (including the optional NVM ES) and by the chip.

6.1.1 TSFs provided by the AXSEAL V2CC Software

SF.SELF_TEST : TOE self _test

This function executes following tests to insure that the TOE is in secure state:

- random number generator test,
- NVM ES integrity test,
- Anti-tearing area integrity test,
- environment sensors check,
- cryptographic operation tests.

Tests could be executed either at initial startup or at dedicated times (execution of sensitive operations).

This function preserves a secure state when failure is detected by TSF.

This function has no strength.

SF.LIFE_CYCLE : Life cycle management

This function manages the lifecycle status and ensures that the status is set in an irreversible way from phase 2 “Manufacturing” to phase 3 “Personalization of the MRTD” and from phase 3 to phase 4 “Operational Use”.

Dedicated commands used by the pre-personalizer for the loading of NVM ES and initialization data are no more available in phases 3 and 4. At the end of phase 3 the BAC mode is enabled and the external authenticate access control is disabled.

In phase 4 after the MRTD application is invalidated by the administrator, data contained in MRTD application are no more available

This function has no strength.

SF.NVMES_LOADING : Loading of the NVM embedded software

This function ensures that NVM ES can be loaded in a secure way onto the TOE in phase 2 “Manufacturing” and that the loading is disabled in an irreversible way when the lifecycle status is set to phase 3 “Personalization of the MRTD”.

This function has no strength.

SF.INTEGRITY : Check of sensitive data integrity

This function checks the integrity of following assets:

- keys (external keys, Basic Access keys, Active authentication key pair),
- Application files (DG1 to DG16, EF.SOD, EF.COM, EF.ICC, EF.DIR),
- NVM ES, anti-tearing area,
- Life cycle status, access rights flags.

SF.INTEGRITY warns the entity connected upon detection of an integrity error of the sensitive data stored within the TSC. Depending on the type of data (user data or TSF data) the TOE enters a secure states or is still available.
This function has no strength.

SF.MUT_AUTH: Identification and Authentication based on mutual authentication

SF.MUT_AUTH allows the authentication of a terminal. This function manages the keys exchanges between the terminal and the TOE. By the way, it provides the means (random generation, TDES encryption, SHA computation) to identify and authenticate the user in a secure way. SF.MUT_AUTH detects each unsuccessful authentication attempt. In such a case it warns the connected terminal. In case of regular termination of the protocol it stores appropriate keys. At the end of the secure messaging session, SF.MUT_AUTH erases securely the session keys.

The strength of this function is high.

SF.SEC_MESS : Data exchange with secure messaging

This function provides the management of the secure channel for the sensitive data exchange with the terminal. A communication channel between the TOE and the Inspection System will be encrypted with a session key, such that the TOE is able to verify the integrity and authenticity of received data (TDES encryption of data and cryptogram computation). The channel is closed in case a wrong cryptogram is received.

This function has no strength.

SF.EXT_AUTH: Identification and Authentication based on external authentication

SF.EXT_AUTH allows the authentication of a terminal by the mean of an external authentication (random generation, cryptogram computation). It detects each unsuccessful authentication attempt. In such a case it warns the connected terminal. The number of allowed authentications may be bounded by a counter.

The strength of this function is high.

SF.INT_AUTH : Authenticity of the MRTD chip

SF.INT_AUTH allows the authentication of the TOE by the terminal by the mean of an internal authentication (RSA signature computation).

This function has no strength.

SF.ACC_CONT: Access Control to stored data objects

SF.ACC_CONT enforces the Security Policies as required in FDP_ACF.1.

This function ensures that the assets (keys, Data Groups, TSF data) can only be accessed under the control of the operating system and as defined by the access rights written during the personalization process. This function also provides the access to the unique identification of the TOE to the administrator (Personalization Agent, Issuing State or Organization) and manages the roles (pre-personalizer, personalizer, user and administrator). This SF controls the reading and writing access in pre-personalization, personalization (External Authenticate Access Control) and user phases (Basic Access Control).

This function has no strength.

SF.PROT_SENS_DATA : Protection of sensitive data

SF.PROT_SENS_DATA provides several mechanisms ensuring the confidentiality of sensitive data during their manipulation. These mechanisms counter the exploitation of electrical or electromagnetic emissions which are generated during the treatment of data.

This function has no strength.

6.1.2 TSFs provided by the P5CD072V0Q Philips chip

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR]. The IC and its primary embedded software is evaluated at level EAL 5 with a minimum strength level for its security functions of SOF-high.

F.RNG : Random Number Generator

This function (random number generation) continuously produces random numbers with a length of one byte.

F.HW_DES : Triple-DES Co-processor

This function provides the Triple Data Encryption Algorithm (TDEA) according to the Data Encryption Standard (DES).

F.OPC : Control of Operating Conditions

This function ensures the correct operation of the TOE during the execution of the IC Dedicated Support Software and Smartcard Embedded Software. This includes all specific security features of the TOE which are able to provide an active response.

F.PHY : Protection against Physical Manipulation

This function protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Software in the ROM, (iii) the Smartcard Embedded Software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM including the configuration data in the security row. It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

F.LOG : Logical Protection

This function implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals.

F.COMP : Protection of Mode Control

This function provides a control of the CPU mode for (i) Boot Mode, (ii) Test Mode and (iii) Mifare Mode. This includes the protection of electronic fuses stored in a protected memory area, the so-called “Security Row”, and the possibility to store initialisation or prepersonalisation data in the so-called “FabKey Area”.

F.MEM_ACC : Memory Access Control

This function controls access of any subject (program code comprising processor instructions) to the memories of the TOE through the Memory Management Unit (MMU).

F.SFR_ACC : Special Function Register Access Control

This function controls access to the Special Function Registers and the switch between the CPU modes.

6.2 ASSURANCE MEASURES

Assurance Measure	Document title
AM_ASE	Axseal Security Target
AM_ADV_FSP	Functional Specifications Axseal
AM_ALC	Class ALC Axseal
AM_ACM	Class ACM Axseal
AM_ADO	Class ADO Axseal
AM_ADV_HLD	High Level Design Axseal
AM_ADV_LLD	Low Level Design Axseal
AM_AGD_ADM	Administrator Guidance Axseal
AM_AGD_USR	User Guidance Axseal
AM_ATE	Class ATE Axseal
AM_AVA_MSU	Misuse Axseal
AM_VLA_SOF	Vulnerability analysis – SOF Axseal
AM_CODE	Source Code for Axseal

Table 6-1 Assurance Measures

The developer team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation. The security of the configuration management is described in detail in a separate document.

The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

The correspondence of the Security Functional Requirements (SFR) with less abstract representations will be demonstrated in a separate document. This addresses ADV_FSP, ADV_HLD, ADV_LLD. ADV_IMP and ADV_RCR.

The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life cycle model of the TOE. The development tools are well defined and documented.

The Gemalto R&E organization is equipped with organizational and personnel means that are necessary to develop the TOE.

As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

7. PP CLAIMS

7.1 PP REFERENCE

The Axseal security target is conformant with the Protection Profile “Machine Readable Travel Document with ICAO Application, Basic Access Control” BSI-PP-0017 version 1.0.

7.2 PP TAILORING

The main refinements and tailoring operated on the PP are:

- This security target does not address the Primary Access Control. The Basic Access Control is implemented and cannot be disabled.
- A new actor MRTD administrator is introduced in phase 4 Operational use for the management of the product.
- Subject Terminal provides administration functionalities (Administration Terminal).
- Threat T.ABUSE_FUNC is refined to address the abuse of administration commands.
- Objective OE.EXAM_MRTD is refined to address the Active Authentication mechanism.
- Objective OE.SECURE_HANDLING is newly specified for the present ST.

Following security functional requirements are refinement or iteration from the PP:

- FMT_MOF.1 Management of security functions behaviour.
- FMT_SMF.1 Specification of management functions.
- FMT_SMR.1 Security roles.
- FMT_MTD.1/INI_READ Management of TSF data.
- FPT_EMSEC.1 TOE Emanation.
- FPT_FLS.1 Failure with preservation of secure state.
- FPT_TST.1 TSF testing.
- FPT_PHP.3 Resistance to physical attack.
- FIA_API.1/SYM_AT Authentication proof of identity.

Following security functional requirements are iteration of existing SFR for the phase 3 “Personalization”:

- FDP_ACC.1/AUTH Subset access control - External authentication access control.
- FDP_ACF.1/AUTH Security attribute based access control - External authentication access control.

Following security functional requirements are iteration of existing SFR for the support of Active Authentication:

- FCS_COP.1/RSA_AA Cryptographic operation.
- FIA_API.1/MRTD Authentication proof of identity.

7.3 PP ADDITIONS

Additions to the PP are items related either to the Active Authentication Mechanism or to the product administration.

For that purpose, two kinds of terminals have to be added: Extended Terminals and Administration Terminals.

Additional threat is added: T.CLONING (related to asset D.MRTD : Authenticity of the MRTD's chip).

Following assumptions are added:

- A.SIGNATURE_PKI: PKI for Passive Authentication,
- A.AUTH_PKI: Inspection Systems for global interoperability,
- A.HOLDER_BEHAV: Behavior of the MRTD Holder.

Additional security objectives and requirements are added for the administration of the product and for the Active Authentication support.

Following security objectives for the TOE are added:

- OT.CHIP_AUTH_PROOF: Proof of MRTD'S chip authenticity
- OT.ADMINISTRATION : Availability of administrative commands in operational use

Following security objectives for the environment are added:

- OE.AUTH_KEY_MRTD: MRTD Authentication Key
- OE.ADMINISTRATION : Administration of logical MRTD

Following security functional requirements are added:

- FAU_ARP.1 Security alarm, dependencies: FAU_SAA.1 Potential violation analysis.
- FDP_RIP.1 Subset residual information protection, no dependencies.
- FDP_SDI.2 Stored data integrity monitoring and action, no dependencies.
- FIA_AFL.1 Basic authentication failure handling, dependencies: FIA_UAU.1 Timing of authentication.
- FIA_ATD.1 User attribute definition, no dependencies.
- FMT_MSA.1 Management of security attributes, dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles.
- FMT_MSA.2 Secure security attributes, dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control], FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles.

8. RATIONALES

Rational is delivered separately only on customer request.

8.1 SECURITY OBJECTIVES RATIONALE

Not delivered in public version

8.2 SECURITY REQUIREMENTS RATIONALE

Not delivered in public version

8.3 TOE SUMMARY SPECIFICATION RATIONALE

Not delivered in public version

8.4 PP CLAIMS RATIONALE

This Security Target is conformant with the Protection Profile “Machine Readable Travel Document with ICAO Application, Basic Access Control”

Main refinements and additions of the present Security Target are the following ones:

- Delivery of the TOE after pre-personalization phase: the TOE is delivered to the personalization agent as a chip with an antenna on an inlay. This is not a passport and all the applicative files have to be written during personalization phase. At TOE delivery there is no MRZ available.
- Configuration with Basic Access Control only: the Axseal product is specified only for use with BAC as the customers are requiring confidentiality for the user data.
- Proof of authenticity with Active Authentication mechanism on Extended Inspection terminal: this functionality adds an advantage for the product security as it forbids the fabrication of a clone.
- Administration in phase 4 “Operational use”: Customer (Issuing state or organization) is requiring dedicated commands for the administration during operational use (invalidation of the MRTD application, maintenance and reliability tracking through the CPLC data).