E-passport 72K

V1.0

Public **S**ecurity **T**arget

TABLE DES MATIERES

TABLE OF FIGURES

1 ST INTRODUCTION

1.1 ST IDENTIFICATION

Title: E-PASSPORT Security Target Public V1.0
FQR 110 3674

Reference:
ROM: EV4/T0QE1040
TOE name: ID One ePass 64K
TOE version : 1.0
Microcontroller: Philips Smart MX P5CD072 V0Q and VOP
Customer ROM code Identification : LDS 1.7 72K V1.0 RC
TOE reference IC + ROM mask 12NC: - 9352 831 41006 VOP
12NC: - 9352 831 64 118 VOQ
TOE documentation:
- SRS
- BISON ADMINISTRATION GUIDANCE

Configuration Management label (PVCS): FINAL_LDS1_7_72K_VERSION_1_0

This Security Target deals with the evaluation of the application software, as well as the composition with the evaluation of the Integrated Circuit (IC). It claims the Protection Profile ICAO BAC [22], and extends it with the Active Authentication mechanism [7].
This security target refers to the micro-controller MX P5CD072 security target [25] that is compliant to BSI 0002 Protection Profile [20].

The Basic Access Control (BAC) mechanism and the Active Authentication (AA) mechanism are optional.

The TOE comprises 2 differents configurations at the end of phase 2:
- If the BAC mode is active at the end of Phase 2, then during phase 3 the BAC mode can not be disable. Phase 4 the BAC mode is active.
- If the BAC mode is not active at the end of Phase 2, then during phase 3 the BAC mode can be activate or not by the personalizer. Phase 4 the BAC mode is active or not according to phase 3.

For additional information see the [SRS] about the EEPROM configuration for masking.

To Sum up in phase 4 the configuration possible are describe below:

TOE configurations	Basic Access Control (BAC)	Active Authentication (AA)
MRTD with BAC	Yes	No
MRTD with BAC and AA	Yes	Yes

The product supports other mechanisms that are used solely for internal usage of Oberthur Card Systems:
- "test mode" allowing access to special functions for testing. Note that the test mode is only suitable for internal usage to make easier the test activity of the product.
- "debrayed mode" allowing quicker personalization by avoiding an authentication for each personalization command.
- A secure mechanism for loading optional code (patches)

The standard cards (mass production) that are delivered to the final customer have the test mode irreversibly deactivated during pre-personalization. This deactivation is realized by the IC manufacturer during pre-personalization operation.

In conclusion, the TOE is the e-passport product where test mode is irreversibly deactivated, and without any optional code.
The TOE name will be the ID One ePass 64K dedicated to the e-passport market.

1.2 ST OVERVIEW

This ST defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the Technical reports of the ICAO New Technology Working Group.

This ST is built on [22] and is conformant to this PP. It extends the Protection Profile with the Active Authentication [7].

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 1999, version 2.1, CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation, Part 2: Introduction and general model, August 1999, version 2.1, CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 1999, version 2.1, CCIMB-99-033

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.

2 TOE Description

2.1 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [6] and providing the Basic Access Control according to the ICAO document [7].

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 documentations [26] [28].

2.2 TOE usage and security features for operational use

State or organisation issues MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading.
The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) 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 a issuing State or Organization.

For this security target the MRTD is viewed as unit of
(a) 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
(1) The biographical data on the biographical data page of the passport book,
(2) The printed data in the Machine-Readable Zone (MRZ) and
(3) The printed portrait.
(b) The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [6] 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 optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both
(4) The other data according to LDS (DG5 to DG16) and
(5) The Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and 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 organisational security measures (e.g. control of materials, personalization procedures) [8]. These security measures include the binding of the MRTD's chip to the passport book.
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 [7]. 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 (iii) in authenticity by the Active Authentication mechanism. This security target does not address the Extended Access Control as optional security mechanisms.
The Basic Access Control is a security feature which shall be mandatory supported by the TOE but may be disabled by the Issuing State or Organization. The inspection system (i) reads the printed data in the MRZ, (ii) authenticates them as inspection system by means of keys derived from MRZ data. 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 [7], Annex E, and [6].

The Active Authentication mechanism ensures that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip. For this purpose the chip contains its own Active Authentication RSA Key pair. A hash representation of Data Group 15 Public Key is stored in the Document Security Object (SO_D) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is stored in the chip's secure memory. The TOE supports the loading and generation of the Active Authentication RSA Key pair.

2.3 TOE logical structure

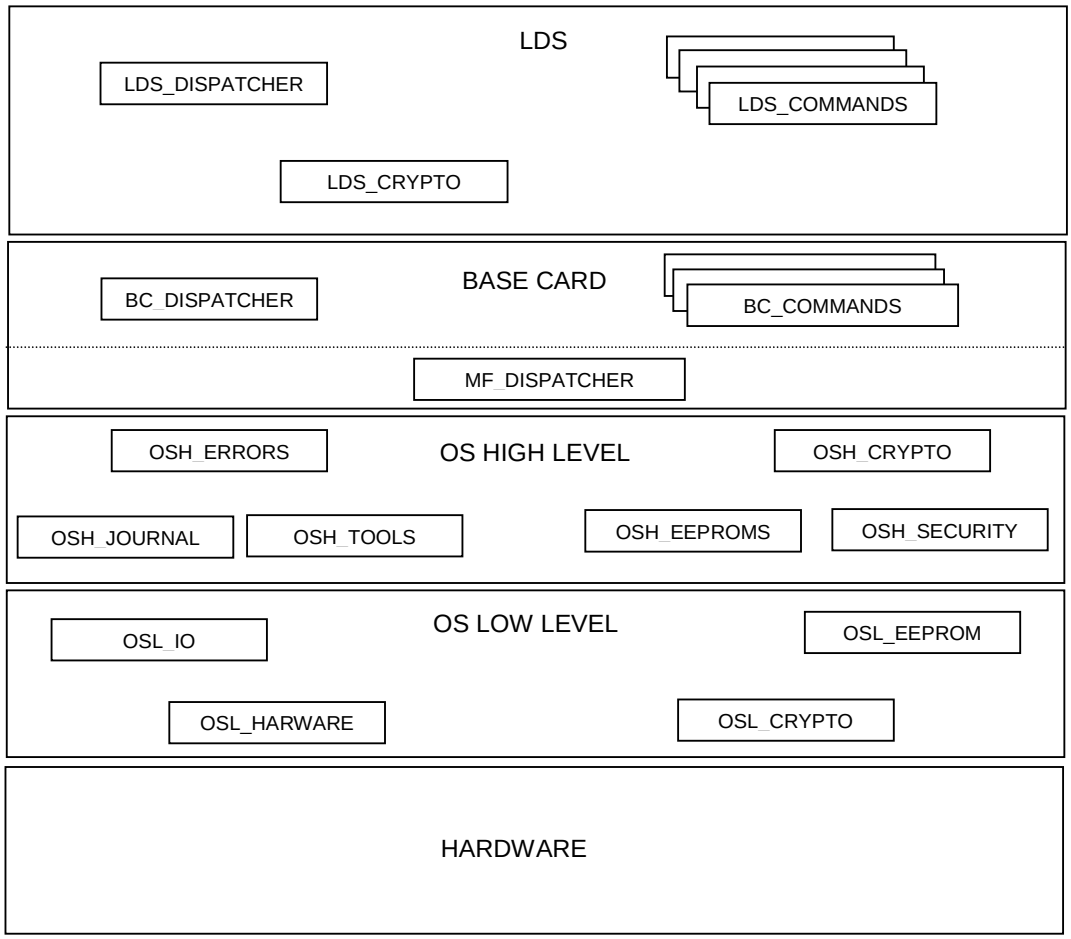

Figure 1 : Logical structure of the TOE

The Figure 1 shows the logical structure of the TOE, showing the layered architecture used to combine the subsystems lightly describe below:

- *LDS: This subsystem fulfils the following functionalities:*
  - *Implements the commands of e-passport that are available in operational phase*
  - *Manages access control on these commands*
  - *Implements authentication mechanisms:*
    - *Basic Access Control (BAC), including session keys generation*
    - *Active Authentication (AA)*
  - *Implements Secure Messaging for received and sent commands*
- *BASE CARD: This subsystem fulfils the following functionalities:*
  - *Implements the commands of e-passport that are available in pre-personalization and personalization phases*
  - *Manages access control on these commands*

- *OS (OS Low level and OS High level): This layer provides an interface between the Hardware and the application layer.*
  - Handle the interface with the Hardware (IC), its security functionality and its different blocks:
    - RAM
    - EEPROM
    - Timer
    - Crypto-processor DES
    - Arithmetic coprocessor (FameX)
    - RNG generator
    - TCL interface
  - *Provides cryptographic support for other layers (LDS and BASE CARD) for the following functionalities:*
    - *3DES (CBC and MAC – based on IC crypto processor)*
    - *random generation (based on IC RNG generator)*
    - *RSA (signature and key generation --- based on FameX co-processor)*
    - *SHA-1*

    It implements self-tests functionality on 3DES, RSA and random generation.
  - *Manages all basic operations (creation, update, read, write, search) on files, on keys, and manages access control on these objects.*
  - *Reacts to security notifications of the IC. These notifications may indicate an attack or an abnormal execution condition.*
  - *Manages Personalizer agent authentication through C-MAC verification*

2.4 TOE life cycle

The TOE life cycle is described in terms of the four 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 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 non-volatile 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 non-volatile 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 manufacture to the MRTD manufacturer.
The MRTD manufacturer (i) add the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary, (ii) creates the MRTD application, and (iii) equips MRTD's chip with Pre-personalization Data.
ST note: The packing process of the IC in the booklet is not done in the manufacturing phase.

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"

ST note: The IC hardware and the antenna are embedded in the booklet during the Personalization phase.

The personalization of the MRTD includes (i) the survey of the MRTD holder biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing the TOE User Data and TSF Data into the logical MRTD and (v) the writing the TSF Data into the logical MRTD and configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (DG1), (ii) the digitised portrait (DG2), and (iii) the Document security object.
The signing of the Document security object by the Document signer [7] 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 1: This security target 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 [7]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organisation, 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 centralised personalization schemes but relies on stronger security protection in the personalization environment (cf. section "Personalization Terminals for further details").

Phase 4 "Operational Use"

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

Application note 2: 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 3: 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.

The delivery of the TOE is at the end of the phase 2.

Phases 1 and 2 are included in the evaluation scope and are covered by configuration management class, life cycle class and delivery assurance class.

Phase 3, the TOE is protected by the security functions. The transfer of TOE between the manufacturer and the personalisation facility is secured.

Phase 4, the security functions are active and protect the TOE.

Precision for phase 2: this part is under the manufacturer responsibility; in addition the TOE is securely transmitted to personalizer for the beginning of phase 3. Everything is managed by the manufacturer.
Precision for phase 3: takes place in the personalisation facility and managed by the Administrator Guidance.

The smartcard product life-cycle is decomposed into 4 phases where the following authorities are involved:

Phase 1	IC design	The IC design is done by NXP. IC Dedicated Software and the guidance documentation are done by NXP.
	E-passport embedded software development	The software developer is Oberthur Card Systems.
	Code Delivery	The Rom Code and EEPROM initialization data are delivered by OCS to NXP
Phase 2	IC Manufacturing	The IC manufacturing is performed on behalf of NXP
	IC Pre Personalization	The IC manufacturer is responsible for the pre-personalization of the TOE.
	IC Testing	The Ic manufacturer performs testing of the TOE
	IC and guidance delivery	The IC is provided by NXP and the guidance is provided to the personalizer by OCS
Phase 3	E-passport printing	The personalizer prints the e-passport and embeds the contactless IC with its antenna in the booklet
	E-passport Personalization	The personalizer is responsible for the E-passport personalization .
	E-passport testing and packaging	The personalizer is responsible for testing and packaging.
Phase 4	E-passport use phase	The E-passport issuer is responsible for the e-passport product delivery to the e-passport holder.

Figure 2 : describes the e-passport product life-cycle.

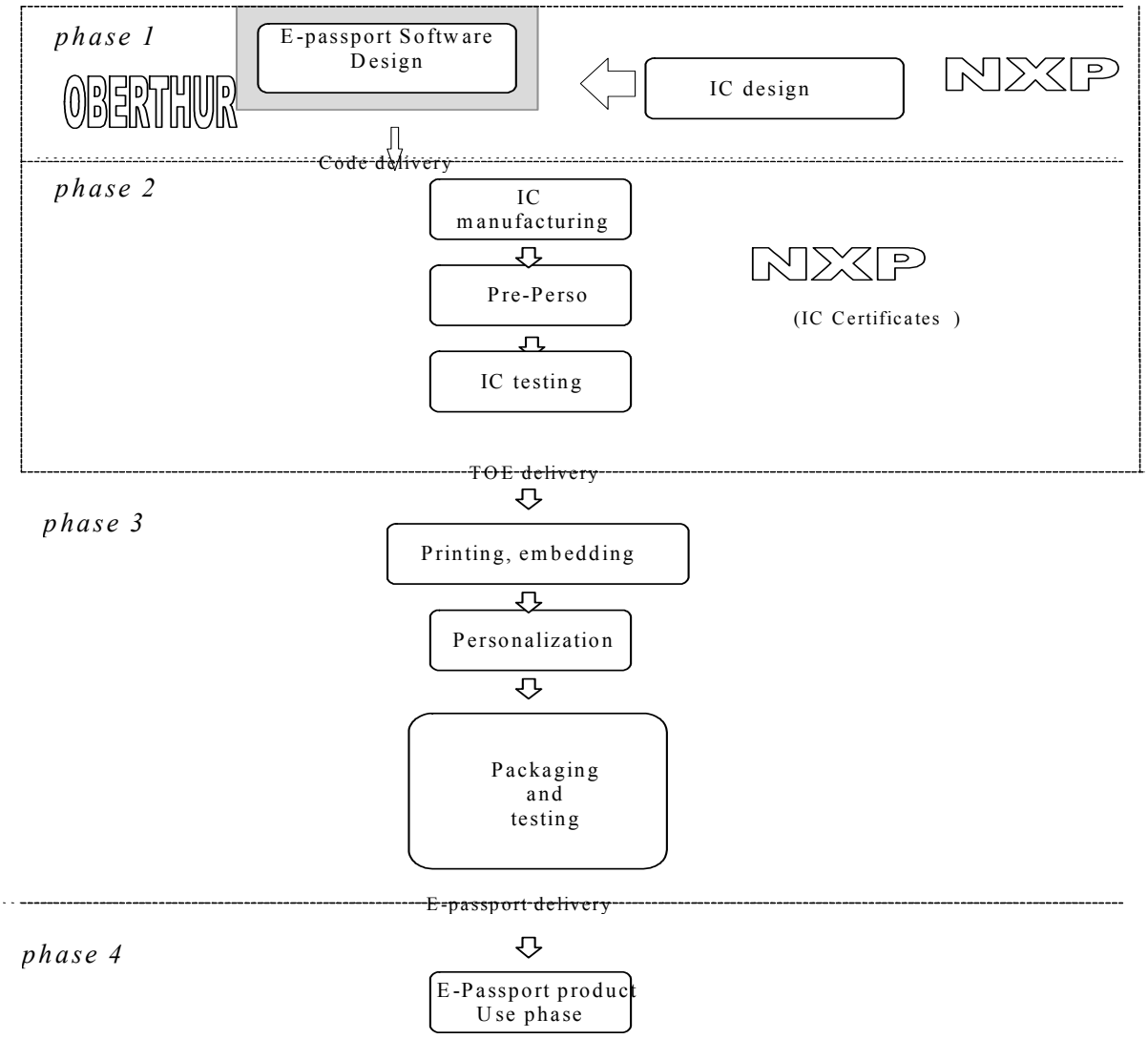

Figure 3 *Smartcard product life-cycle for the TOE*

3 TOE Security Environment

3.1 Assets

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

Logical MRTD Data

The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [6]. 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.

An additional asset is the following more general one.

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 traveller 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 personalised the MRTD.

Traveller
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 Organisation to personalize the MRTD for the holder by some or all of the following activities (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) and/or the encoded iris image(s) (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability and (iv) signing the Document Security Object defined in [6].

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.

The **Primary Inspection System** (PIS) (i) contains a terminal for the contact less communication with the MRTD's chip and (ii) 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) (i) contains a terminal for the contact less communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) 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 (i) implements the Active Authentication Mechanism, (ii) supports the terminals part of the Extended Access Control Authentication Mechanism and (iii) is authorized by the issuing State or Organization to read the optional biometric reference data.

Application note 4: This security target does not distinguish between the BIS and EIS because the Extended Access Control is outside the scope. Only the BIS as part of EIS is in the scope of this evaluation.

Terminal
A terminal is any technical system communicating with the TOE through the contact less interface.

Attacker
A threat agent trying (i) to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD

Application note 5: 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.

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 traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [7]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

- **Application note 6**: According to [7] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of this security target the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read the logical MRTD if the logical MRTD is protected by Basic Access Control. The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems. The Active authentication is also optional and can be enabled or disabled by the Personalization agent**.**

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 contact less communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.Skimming Skimming the logical MRTD
An attacker imitates the inspection system to read the logical MRTD or parts of it via the contact less 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.

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 holders 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 an other identity of the traveller. The attacker may alter the printed portrait and the digitised 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 digitised portrait and optional biometric reference data of finger read from the logical MRTD of a traveller 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 an other contact less chip.

The TOE shall avert the threat as specified below.

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 initialisation and the personalization in the operational state after delivery to MRTD holder.

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 contact less interface (emanation) or direct measurements (by contact to the chip still available even for a contact less 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 pre-requisite. 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.

T.Counterfeit MRTD's chip

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveller by possession of a MRTD.

The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

3.5 Organisational Security Policies

The TOE shall comply to the following organisation security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation 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 Initialisation 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 digitised 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 digitised 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 [7]. The issuing State or Organization decides (i) to enable the Basic Access Control for the protection of the MRTD holder personal data or (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD.

Application note 7: The organisational security policy P.Personal_Data is drawn from the ICAO Technical Report [7]. 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 organisational 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 [6] 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 8:The OT.AC_Pers implies that
(1) 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,
(2) 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. If the TOE is configured for the use with Primary Inspection Systems no protection in confidentiality of the logical MRTD is required.

Application note 9: The traveller 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 [7] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf (Cf. CEM [4], section 8.10.3.4, paragraph. 1625).

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 an 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 10: 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 tractability 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 contact less interface before successful authentication as Basic Inspection System or as Personalization Agent.

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 (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smart card Embedded Software, (iii) to manipulate Soft-coded Smart card Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

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

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 and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Application note 11: 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) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

With a prior

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

Application note 12: 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 13: 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.Chip_Authenticity Protection against forgery
The TOE must support the Inspection Systems to verify the authenticity of the MRTD's chip. The TOE stores a RSA private key to prove its identity, and that is used in chip authentication. This mechanism is described in [7] as "Active Authentication".

4.2 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 Initialisation 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 permutation 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 initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.3 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 Organisation (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 [6].

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 traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD.

OE.Passive_Auth_Verif Verification by Passive Authentication
The border control officer of the Receiving State uses the inspection system to verify the traveller 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 14: The Primary Inspection System may prevent unauthorized listening to or manipulation of the communication with the MRTD's chip e.g. by a Faraday cage.

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.

MRTD Holder

OE.Secure_Handling Secure handling of the MRTD by MRTD holder
The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contact less interface.

Application note 15: The MRTD holder may prevent unauthorized communication of the MRTD's chip with terminals e.g. by carrying the MRTD in a metal box working as Faraday cage.

5 Security Requirements

5.1 Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [20], other components are defined in this security target.

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.

FAU_SAS Audit data storage 1
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: *authorised 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.

FCS_RND Generation of random numbers	1

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

97 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 the 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 16: 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 that this security target 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".

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.

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.

FMT_LIM Limited capabilities and availability

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 lifecycle.

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 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 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 17: 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 (i) 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 (ii) 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 [2].

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

Family behaviour
This family defines requirements to mitigate intelligible emanations.

FPT_EMSEC TOE emanation 1

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 emits 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

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

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide the ***Manufacturer*** with the capability to store ***the IC Identification Data*** in the audit records.
Dependencies: No dependencies.

Application note 18: 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 Initialisation 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 fulfil the security objective OD.Assurance.

5.2.2 Class Cryptographic Support (FCS)

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.

5.2.2.1 Cryptographic key generation (FCS_CKM.1)

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 Key Derivation Algorithm*** and specified cryptographic key sizes ***112 bit*** that meet the following: ***[7], Annex E***.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 19: 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 [7], 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 [7], 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 Cryptographic key destruction - MRTD

FCS_CKM.4.1/ MRTD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***irreversible logical erasing*** that meets the following: ***no standard***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2
Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

Application note 20: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

Cryptographic operation (FCS_COP.1)

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.1.1/RSA_MRTD Cryptographic operation – RSA signature by MRTD

The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **RSA with SHA-1** and cryptographic key sizes **1024 bits** that meet the following: **scheme 1 of ISO/IEC 9796-2:2002**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

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: ***FIPS 180-2***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 21: 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/BAC_MRTD) according to [7].

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 bit*** that meet the following: ***FIPS 46-3 [14] and [7]; Annex E***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 22: 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 FCS_CKM.1/BAC_MRTD and 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.

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 bit*** that meet the following: ***ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 23: 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/BAC_MRTD.

Random Number Generation (FCS_RND.1)

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, following AIS 31 [27].**

Dependencies: No dependencies.

Application note 24: 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 FIA Identification and Authentication

Application note 25: The Table 1 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 [7], Annex E, and [23]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD and FIA_UAU.6/MRTD	FIA_UAU.4/BT and FIA_UAU.6/T	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Active Authentication Mechanism	FIA_API.1/AA	FIA_UAU.4/BT	RSA with 1024 bits. Algorithm according to [7], Annex D.

Table 1: Overview on authentication SFR

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow
(1) To read the Initialisation Data in Phase 2 "Manufacturing",
(2) To read the ATS in Phase 3 "Personalization of the MRTD",
(3) To read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",
(4) To read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 "Operational Use"
on behalf of the user to be performed before the user is identified.

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

Dependencies: No dependencies.

Application note 26: The IC manufacturer and the MRTD manufacturer write the Initialisation 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 Primary Inspection System s any terminal is assumed as Primary Inspection System and is allowed to read the logical MRTD. 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/T.

Application note 27: 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 than 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.
In this Security Target, the chip identifier cannot be read in the operational phase.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow
(1) to read the Initialisation Data in Phase 2 "Manufacturing",
(2) to read the ATS in Phase 3 "Personalization of the MRTD",
(3) to read the ATS if the TOE is configured for use with Basic Inspection Systems only in Phase 4 "Operational Use",
(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 "Operational Use"
on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification.

Application note 28: The Primary Inspection System does not authenticate themselves. Only the Basic Inspection System and the Personalization Agent authenticate themselves.

FIA_API.1/AA Authentication Proof of Identity - MRTD

FIA_API.1.1/AA The TSF shall provide an ***Active Authentication Protocol*** to prove the identity of the TOE.

Dependencies: No dependencies.

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
1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on Triple-DES,

Dependencies: No dependencies.

Application note 29: 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 [7], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.

Application note 30: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [7]. 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 Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide
1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on Triple-DES
to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms
(a) the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
(b) the Symmetric Authentication Mechanism with the Personalization Agent Key
2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
Dependencies: No dependencies.

Application note 31: 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 [7], 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.
In this Security Target, the option (a) of the SFR is not available: Personalisation agent can only be authenticated using the Symmetric Authentication Mechanism with the Personalization Agent Key.

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 ***each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism***.

Dependencies: No dependencies.

Application note 32: The Basic Access Control Mechanism specified in [7] 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.

5.2.4 Class FDP User Data Protection

Subset access control (FDP_ACC.1)

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.

FDP_ACC.1 Subset access control – Primary Access Control

FDP_ACC.1.1/PRIM The TSF shall enforce the ***Primary Access Control SFP*** on ***terminals gaining write, read and modification access to data groups DG1 to DG16 and Active Authentication Private Key of the logical MRTD***.

Dependencies: FDP_ACF.1 Security attribute based access control

Application note 33: The data groups DG1 to DG16 of the logical MRTD as defined in [6] are the only TOE User data. The Primary Access Control SFP addresses the TOE usage with Primary Inspection Systems and Basic Inspection Systems independent on the configuration of the TOE.

FDP_ACC.1 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 and Active Authentication Private Key of the logical MRTD***.

Dependencies: FDP_ACF.1 Security attribute based access control

Application note 34: The Basic Access Control SFP addresses the configuration of the TOE for usage with Basic Inspection Systems only.

Security attributes based access control (FDP_ACF.1)

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.

FDP_ACF.1 Security attributes based access control – Primary Access Control

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

1. Subjects:

a. Personalization Agent,

b. Terminals,

2. Objects: data in the data groups DG1 to DG16 of the logical MRTD, and Active Authentication Private Key

3. Security attributes

a. configuration of the TOE according to FMT_MOF.1,

b. authentication status of terminals.

FDP_ACF.1.2/PRIM
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: i***n the TOE configuration for use with Primary Inspection Systems***

1. the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key

2. the Terminals are allowed to read the data of the groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key.

3. the successfully authenticated Personalization Agent is allowed to write the Active Authentication Private Key

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

FDP_ACF.1.4/PRIM
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***.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

Application note 35: The MRTD access control prevents changes of data groups by write access to the logical MRTD after their creation by the Personalization Agent (i.e. no update of successful written data in the data groups DG1 to DG16). The Passive Authentication Mechanism detects any unauthorised changes.

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

FDP_ACF.1.1/BASIC The TSF shall enforce the Basic Access Control SFP**35** to objects based on the following:

1. Subjects:

a. Personalization Agent,

b. Basic Inspection System,

c. Terminal,

2. Objects: data in the data groups DG1 to DG16 of the logical MRTD and and Active Authentication Private Key

3. Security attributes

a. configuration of the TOE according to FMT_MOF.1,
b. 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: ***in the TOE configuration for use with Basic Inspection Systems only***

1. ***the successfully authenticated Personalization Agent is allowed to write and to read the data of the data groups DG1 to DG16 of the logical MRTD, including the Active Authenticate Public Key***
2. ***the successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG16 of the logical MRT,D including the Active Authenticate Public Key.***
3. ***the successfully authenticated Personalization Agent is allowed to write the Active Authentication Private Key***

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

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***.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

Inter-TSF-Transfer

Application note 36: 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_UCT.1/MRTD Basic data exchange confidentiality - MRTD

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

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FDP_UIT.1/MRTD Data exchange integrity - MRTD

FDP_UIT.1.1/MRTD The TSF 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/MRTD The TSF shall be able to determine on receipt of user data, whether ***modification, deletion, insertion and replay*** has occurred.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

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

This requirement deals with the import of Active Authentication private RSA key, when it is not generated on card. It is applicable for TOE with or without BAC.

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

FDP_ITC.1.2/AA The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: ***none***.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialization

5.2.5 Class FMT Security Management

FMT_MOF.1 Management of functions in TSF

.
FMT_MOF.1.1 The TSF shall restrict the ability to ***enable and disable*** the functions ***TSF Basic Access Control*** and Active Authentication to ***Personalization Agent***.

Dependencies: No Dependencies

Application note 37: The enabling and disabling the TSF Basic Access Control defines the configuration of the TOE in Phase 3 “Personalization of the MRTD” before use in the phase 4 “Operational Use”:

1. The TOE is configured with Primary Inspection systems when the TSF Basic Access Control is disabled. In this configuration the TOE enforces the Primary Access Control SFP according to FDP_ACC.1/PRIM and FDP_ACF.1/PRIM. In this case the logical MRTD may be read without successful authentication as Basic Inspection System or Personalization Agent.
2. The TOE is configured with Basic Inspection Systems only when the TSF Basic Access Control is enabled. In this configuration 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 or Personalization Agent.

It is up to the security target writer to decide whether the disabling of the TSF Basic Access Control is accompanied with the disabling of the Basic Access Control Authentication Mechanism. Even if the TOE will be configured for use in the phase 4 “Operational Use” with Primary Inspection systems the Personalization Agent may use this mechanism with the Personalization Agent Authentication Keys or a Basic Inspection System may use this mechanism together with secure messaging to protect the logical MRTD against eavesdropping to the communication between TOE and inspection system.
In this Security Target, when the BAC mechanism is disabled the Basic Access Control Authentication Mechanism cannot be used with the Personalization Agent keys or any other keys.
Moreover the Active Authentication mechanism can be enabled or disabled by the Personalization Agent.

Application note 38: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

FMT_SMF.1 Specification of Management Functions

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

1. Initialization,
2. Personalization,
3. Configuration

Dependencies: No Dependencies

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Primary Inspection System,
4. Basic Inspection System.

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

Application note 39: 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.

FMT_LIM.1 Limited capabilities

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

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

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.2 Limited availability

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

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

Dependencies: FMT_LIM.1 Limited capabilities.

Application note 40: 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.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialisation Data and Prepersonalisation Data

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

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 41: 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 Initialisation 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 ***Initialisation Data*** to ***the Personalization Agent***.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 42: 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.

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 and the Active Authentication RSA private key*** to ***the Personalization Agent***.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

185 **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, the Active Authentication RSA private key and Personalization Agent Keys*** to ***none***.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 43: The Personalization Agent generates stores and ensures the correctness of the Document Basic Access Keys if the Basic Access Control is enabled. Note the Document Basic Access Keys may be used for the Basic Access Control Authentication Mechanism and secure messaging even if the Basic Access Control is disabled (cf. Application note 37).

5.2.6 Class FPT Protection of the Security Functions

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-bypass ability 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.

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit ***power variations, timing variations during command execution*** in excess of ***non useful information*** enabling access to ***personalization agent Authentication Key***.

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 ***Personalization Agent Authentication Key***.

Dependencies: No other components.

Application note 44: The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. 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 contact less 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.

FPT_FLS.1 Failure with preservation of secure state

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

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests ***at the request of the authorised user*** to demonstrate the correct operation of the TSF.

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

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

Dependencies: FPT_AMT.1 Abstract machine testing.

Application note 45: The ST writer shall perform the operation in FPR_TST.1.1. 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.

198 **FPT_PHP.3 Resistance to physical attack**

FPT_PHP.3.1 The TSF shall resist ***physical manipulation and physical probing*** to the TSF by responding automatically such that the ***TSP*** is not violated.

Dependencies: No dependencies.

Application note 46: 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.

FPT_RVM.1 Non-bypass ability 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.

Dependencies: No dependencies.

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 entrusted subjects.

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

Dependencies: No dependencies.

Application note 47: 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 assurances 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 48: The high minimum strength of function covers the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or per mutational mechanisms are involved, e.g. due to challenges generated by the TOE and sent to the terminal or probabilistic self tests.

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.

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 [7] 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 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.

Dependencies: No dependencies

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 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: ***[7], Annex E***.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 49: The terminals derive the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [7], 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/BAC_MRTD.

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 ***irreversible erasing*** that meets the following: ***no standard***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

Application note 50: The ST writer shall perform the operation in FCS_CKM.4.1/BT. The basic terminal 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 specified cryptographic algorithms ***SHA-1*** and cryptographic key sizes ***none*** that meet the following: ***FIPS 180-2***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 51: 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 bit*** that meet the following: ***FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2)***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 52: 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 s***ecure messaging – message authentication code*** in accordance with a specified cryptographic algorithm ***Retail-MAC*** and cryptographic key sizes ***112 bit***[85] that meet the following: ***FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2)***.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 53: 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 - 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, following AIS 31 [27].**

Dependencies: No dependencies.

Application note 54: The ST writer shall perform the operation in FCS_RND.1.1/BT. 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

1. ***Basic Access Control Authentication Mechanism***.
2. ***Active Authentication Mechanism***

Dependencies: No dependencies.

Application note 55: The Basic Access Control Authentication Mechanism [7] 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 e***ach command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism***.

Dependencies: No dependencies.

Application note 56: The Basic Access Control Mechanism specified in [7] 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 57: 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 ***BT part of Basic Access Control SFP*** to be able to ***transmit and receive*** objects in a manner protected from unauthorised disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UIT.1/BT Data exchange integrity - Basic Terminal

FDP_UIT.1.1/BT the **Basic Terminal** shall enforce the ***BT part of 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.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.4.3 Personalization Terminals

242 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 listen or manipulated.

(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.

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 a ***Authentication Mechanism based on Triple-DES*** to prove the identity of the ***Personalization Agent***.

Dependencies: No dependencies.

Application note 58: 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 [24] 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).

FCS_CKM.1/PERSO Cryptographic key generation – Generation of Active Authenticate Keys

This SFR deals with RSA key generation for Active Authentication when they are generated off card and imported into the card.

FCS_CKM.1.1/ AA_MRTD the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***RSA key generation*** and specified cryptographic key sizes ***1024 bits*** that meet the following: ***ANSI X9.31 [18].***

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.4.4 Terminal with Active Authentication feature

FCS_RND.1/AA Quality metric for random numbers

FCS_RND.1.1/AA 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, following AIS 31 [27].**

Dependencies: No dependencies.

FCS_COP.1/RSA_AA Cryptographic operation – RSA signature

FCS_COP.1.1/RSA The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **Public RSA with SHA-1** and cryptographic key sizes **1024 bits** that meet the following: **scheme 1 of ISO/IEC 9796-2:2002**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

6 TOE SUMMARY SPECIFICATION

The minimum strength of function is SOF-high.

F.ACC_READ Access Control in reading
This function controls access to read functions depending on user, authentication status and card lifecycle.

1. In the operational use:
   - When the BAC mechanism is active in the card, The terminal can read user data, the Document Security Object and Active Authentication Public key after BAC authentication
   - When the BAC authentication mechanism is not active in the card, The terminal can read user data, the Document Security Object and Active Authentication Public key without authentication
   - ICC identification cannot be read in this phase

2. In the personalisation phase:
   - The personalisation agent can read user data, the Document Security Object and Active Authentication Public key after symmetric authentication
   - ICC identification can be read in this phase

3. In all phases, BAC keys, Active Authentication private key and Personalisation agent keys cannot be read.

F.ACC_WRITE Access Control in writing

This function controls access to write functions depending on user, authentication status and card lifecycle.
The configuration locks defined some security part active in the card such as BAC mode, Active Authenticate mode. These locks are used for internal check and determine the configuration of the TOE in use phase.

1. In the personalisation phase:
   - user data, the Document Security Object, BAC keys, Active Authentication keys and Personalisation Agent keys after symmetric authentication can be written in this phase, LDS configuration lock can be written

2. In the operational use:
   - user data, the Document Security Object, BAC keys, Active Authentication keys and Personalisation Agent keys cannot be written in this phase

F.BAC BAC mechanism
BAC mechanism [7] is used during operational phase to authenticate the terminal; this protocol generates the session keys to be used for secure messaging. Sessions keys are destroyed at the BAC session closure. A self-test on TDES and random generator is performed when a BAC session is requested.

SOF Claim:
- BAC mechanism is SOF-High.

F.SM Secure Messaging
After BAC authentication, a private communication is established based on TDES CBC and Retail MAC algorithms. This channel protects in integrity and confidentiality of commands exchanged between the terminal and the card.

F.AUTH_PERSO Personalisation Agent Authentication
The personalisation agent is authentication using Symmetric Authentication mechanism based on 3DES Retail MAC.

F.AA Active Authentication
This security function performs the Active Authentication as described in [7]. A self-test on RSA and random is performed when an Active Authentication is requested.

SOF Claim:
- Active Authentication mechanism is SOF-High.

IC Security Functions:

We give here the security functions of the IC. In this description, the term TOE means IC.
The complete description is available in [25].
IC Security Target [25] made a SOF claim “high” (SOF-HIGH) for all IC functions that are realized by probabilistic or per mutational mechanisms: F.RNG, F.LOG, F.HW_DES.

F.RNG: Random Number Generator
The random number generator continuously produces random numbers with a length of one byte. The TOE implements the F.RNG by means of a physical hardware random number generator working stable within the limits guaranteed by F.OPC (operational conditions).
The TSF provides a hardware test functionality that can be used by the Smart card Embedded Software to detect faults in the hardware implementing the random number generator.

F.HW_DES: Triple-DES Co-processor

The TOE provides the Triple Data Encryption Algorithm (TDEA) according to the Data Encryption Standard (DES). F.HW_DES is a modular basic cryptographic function which provides the TDEA algorithm as defined by FIPS PUB 46 by means of a hardware co-processor and supports (a) the 3-key Triple-DEA algorithm according to keying option 1 and (b) the 2-key Triple DEA algorithm according to keying option 2 in FIPS PUB 46-3 [131. The two/three 56 bit keys (112/168 bit) for the 2-key/3-key Triple DES algorithm shall be provided by the Smart card Embedded Software. For encryption the Smart card Embedded Software provides 8 bytes of the plain text and F.HW_DES calculates 8 bytes cipher text. The calculation output is read by the Smart card Embedded Software. For decryption the Smart card Embedded Software

F.OPC: Control of Operating Conditions
The function F.OPC ensures the correct operation of the TOE (functions offered by the micro controller including the standard CPU as well as the Triple-DES co-processor, the arithmetic coprocessor, the memories, registers, I/O interface and the other system peripherals) during the execution of the IC Dedicated Support Software and Smart card 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
The function F.PHY protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Software in the ROM, (iii) the Smart card 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
The function F.LOG 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. This comprises the power consumption and signals on the other pads that are not intended by the terminal or the Smartcard Embedded Software. Thereby this security function prevents the disclosure of User Data or TSF data stored and/or processed in the smartcard IC through the measurement of the power consumption and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other security functions.

F.COMP: Protection of Mode Control
The function F.COMP 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 initialization or pre-personalization data in the so-called "FabKey Area".

F.MEM ACC: Memory Access Control
F.MEM ACC controls access of any subject (program code comprising processor instructions) to the memories of the TOE through the Memory Management Unit (MMU). Memory access is based on virtual addresses that are mapped to physical addresses. The CPU always uses virtual addresses. The Memory Management Unit performs the translation from virtual to physical addresses and the physical addresses are provided from the MMU to the memory interfaces to access the memories. The access control is performed in two ways:

F.SFR ACC: Special Function Register Access Control
The function F.SFR ACC controls access to the Special Function Registers and the switch between the CPU modes.

6.1 Assurance measures EAL4+

Requirement	Measures	Reference
Configuration management		
ACM_AUT.1	Partial CM automation	• Méthodologie de Gestion de configuration • Gestion des documents • Génération et archivage • OCS R&D change management • Bison Configuration List
ACM_CAP.4	Generation support and acceptance procedure	
ACM_SCP.2	Problem tracking CM coverage	
Life cycle support		
ALC_DVS.2	Sufficiency of security measures	• Processus développement des produits • Sécurité physique et accès des personnes au site OCS de Nanterre • Global Security Policy • Global IT Security Policy (public version) • Procédure de gestion des cartes de test • Règles d'établissement et de gestion des engagements de confidentialité • Rules for protection of sensitive information
ALC_LCD.1	Developer defined life-cycle mode	
ALC_TAT.1	Well defined development tools	
Delivery and operation		
ADO_DEL.2	Detection of modification	• Transfert sécurisé des masques et codes optionnels • Philips Entry Order Form (Masking order) • Application LDS 1.7 72K on P5CD072 - INSTRUCTIONS DE GENERATION DU LOGICIEL
ADO_IGS.1	Installation, generation and start-up procedures	
Development		
ADV_FSP.2	Fully defined external interfaces	• BISON FSP SPM • SRS • PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1 Date - October 01, 2004
ADV_HLD.2	Security enforcing high level design	• BISON HLD LLD

Requirement	Measures	Reference
ADV_LLD.1	Security enforcing low level design	• BISON HLD LLD
ADV_IMP.2	Implementation of the TSF	• Code source
ADV_RCR.1	Informel correspondance démonstration	• BISON FSP_SPM • BISON HLD LLD
ADV_SPM.1	Informal TOE security policy model	• BISON FSP_SPM • SRS
Guidance document		
AGD_ADM.1	Administrator Guidance	• BISON AGD • SRS
AGD_USR.1	User guidance	
Tests		
ATE_COV.2	Analysis of coverage	• BISON ATE • Tests scripts
ATE_DPT.1	Testing high-level design	
ATE_FUN.1	Functional testing	
ATE_IND.2	Independent testing sample	• TOE Samples
Vulnerability assessment		
AVA_MSU.2	Validation of guidance analysis	• BISON MSU
AVA_SOF.1	Strength of the TSF evaluation	• BISON SOF
AVA_VLA.2	Highly resistant : Construction vulnerability Usage vulnerability	• BISON VLA • TOE Samples

7 PP CLAIMS

7.1 PP reference

The PP ICAO BAC [22] is claimed.

7.2 PP refinements

Non applicable

7.3 PP additions

The additional functionality is the Active Authentication (AA) based on the ICAO PKI V1.1

8 PP Claim Rationale

This security target is conforming to the ICAO BAC Protection Profile [22]. In addition the Active Authentication mechanism is included in the TOE. It implies some augmentations that are described below.

Addition of new Threats:

- T.Counterfeit

Addition of new TOE Objectives:

- OT.Chip_Authenticity

Addition of new IT Environment Objectives:

- OE.Auth_Key_MRTD

Addition of new SFRs for the TOE:

- FCS_COP.1.1/RSA_MRTD
- FDP_ITC.1/AA
- FIA_API.1/AA

Extension of existing SFRs for the TOE: It consists in an addition in the refinement of the SFR to include data pertaining to Active Authentication mechanism.

- FDP_ACC.1/PRIM and FDP_ACF.1/PRIM: to include Active Authenticate Public and Private Keys in the managed data
- FDP_ACC.1/BASIC and FDP_ACF.1/BASIC: to include the Active Authenticate Public and Private Keys in the managed data
- FMT_MOF.1: add the configuration of Active Authentication that is restricted to the Personalization Agent.
- FMT_MTD.1/KEY_WRITE: extension of this SFR to include the Active Authentication RSA private key
- FMT_MTD.1/KEY_READ: extension of this SFR to include the Active Authentication RSA private key

Addition of new IT environment SFRs:

- FCS_CKM.1/PERSO
- FCS_RND.1/AA
- FCS_COP.1.1/RSA

Extension of IT environment SFRs:

- FIA_UAU.4/BT: include the Active Authentication mechanism

9 Literature

Common Criteria
[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1, August 1999

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

[5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

ICAO

[6] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[7] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[8] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[9] 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 1.9, ICAO TAG MRTD/NTWG, 19 May 2003

[10] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

[11] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version – 0.42 - Draft, August, 2004, Dr. Kügler, BSI

Cryptography

[12] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Bonn, 10.8.2004 (Zieldatum der Veröffentlichung ist Januar 2005)

[13] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[14] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

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

[16] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[17] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

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

[19] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

Protection Profiles

[20] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[21] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[22] Machine Readable Travel Document with „ICAO Application", Basic Access Control BSI-PP-0017, 18 August 2005, Version 1.0

Other

[23] Technical Report Advanced Security Mechanisms for Machine Readable Travel Documents, Version 0.8 (final), BSI

[24] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004

[25] Security Target Lite BSI-DSZ-CC-0349 -- Evaluation of the Philips P5CT072V0Q, P5CD072V0Q and P5CD036V0Q Secure Smart Card Controllers, Version 1.2, January 13th, 2005

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