TÜBİTAK BİLGEM UEKAE
ULUSAL ELEKTRONİK & KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

AKİS PROJESİ

AKİS-PASAPORT
SECURITY TARGET-LITE

AKİS V1.4i

Revision No	07
Revision Date	24.06.2013
Document Code	AKIS-ST
File Name	AKIS_PASAPORT_ST.DOC

Prepared by	
Fehime BIYIKLIOĞLU	Mehtap KARAMANLI
Mehmet ERİŞ	
Approved by	
Project Manager	Yrd. Doç. Dr. Ercan ÖLÇER

Date of Revision

Revision No	Revision Reason	Date of Revision
01	First Publication	20.09.2011
02	OR1 Corrections	20.04.2012
03	GR2 Corrections	25.05.2012
04	GR4 Corrections	20.07.2012
05	GR9 Corrections	27.11.2012
06	GR10 Corrections	02.03.2013
07	GR13 Corrections	24.06.2013

CONTENT

LIST OF FIGURES

LIST OF TABLES

Glossary&Abbreviations

AKiS	**Akıllı Kart İşletimSistemi**
ACE	**Advanced Crypto Engine**
APDU	**Application Protocol Data Unit**
CC	**Common Criteria**
DF	**Dedicated File**
DG	**Data Group**
EAL	**Evaluation Assurance Level**
EF	**Elemantary File**
ES	**Embedded Software**
ICAO	**International Civil Aviation Organization**
ICCSN	**Integrated Circuit Serial Number**
MRTD	**Machine Readable Travel Document**
MF	**Master File**
NVM	**Non Volatile Memory**
OS	**Operating System**
ST	**Security Target**
TOE	**Target of Evaluation**
TPDU	**Transmission Protocol Data Unit**
TSF	**TOE Security Functionality**

Table 1Abbreviations & Glossary

Basic Software: Itis the part of ES in charge of the generic functions of the Smartcard IC such as Operating System, general routines and Interpreters.
Embedded Software: It is defined as the software embedded in the Smartcard Integrated Circuit. The ES may be in any part of the non-volatile memories of the Smartcard IC.
Embedded software developer: Institution (or its agent) responsible for the smartcard embedded software development and the specification of pre-personalization requirements.
Initialization: Itis the process to write specific information in the NVM (Non-Volatile Memory) during IC manufacturing and testing (smartcard product life cycle phase 3) as well as to execute security protection procedures by the IC manufacturer. The information could contain protection codes or cryptographic keys.
Integrated Circuit (IC): Electronic component(s) designed to perform processing and/or memory functions.
IC designer: Institution (or its agent) responsible for the IC development.
IC manufacturer: Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.
IC packaging manufacturer: Institution (or its agent) responsible for the IC packaging and testing**.**
Personalizer: Institution (or its agent) responsible for the smartcard personalization and final testing.
Personalization data: Specific information in the non volatile memory during personalization phase.
Security Information: Secret data, initialization data or control parameters for protection system.
Smartcard: A credit sized plastic card which has a non volatile memory and a processing unit embedded within it.

Smartcard Issuer: Institution (or its agent) responsible for the smartcard product delivery to the smartcard end-user.

Smartcard product manufacturer: Institution (or its agent) responsible for the smartcard product finishing process and testing.

1. SECURITY TARGET INTRODUCTION

1.1 ST Reference

ST Title: AKiS-Pasaport v1.4i Security Target, rev 7, 24.06.2013

This Security Target describes the TOE, intended IT environment (terminal, inspection system, and basic inspection system), security objectives, security requirements, security functions and all necessary rationale.

1.2 TOE Reference

TOE Identification: AKiS-Pasaport v1.4i

1.3 TOE Overview

1.3.1 TOE definition

AKiS-Pasaport v1.4i is a smart card which is designed to be used as Machine Readable Travel Document (MRTD). The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel document (AKiS-Pasaport) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303'.

1.3.2 TOE usage and security features for operational use

The usage and security features are as defined in the MRTD with ICAO Application, Basic Access Control protection profile:
A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST 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 traveler 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) optional biometrics using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

1.3.3 Non-TOE hardware/software/firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.4 TOE Description

AKiS v1.4i algorithms and crypto specifications are;

Communication
ISO/IEC 14443 Identification Cards – Contactless Integrated Circuit Cards

Basic Access Control;
ISO/IEC11770-2 Key Establishment Mechanism 6
3DES CBC as block cipher
Cryptographic checksum ISO/IEC9797-1 MAC Algorithm 3

Active Authentication;
ISO/IEC9796-2 Digital Signature Scheme 1

1.4.1 Physical Scope of TOE

The TOE comprises

- the circuitry of the MRTD's chip (the integrated circuit, IC): IFX SLE78CLFX1600PM the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (AKiS-Pasaport v1.4i OS),
- the MRTD application and
- the MRTD User Manual

1.4.1.1 MRTD Chip

The integrated circuit of the MRTD's chip is IFX SLE78CLFX1600PM. IFX SLE78CLFX1600PMhasCC EAL 5+ (AVA_VAN.5, ALC_DVS.2) certificate. AKiS-Pasaport v1.4i Operating System is loaded into the Flash Memory of the IFX chip (that is set as Read Only – chip: SLE78CLFX1600PM) during the manufacturing of the IC.

1.4.1.2 AKiS v1.4i Operating System

Smart cards are used as electronic authentication keys, digital signs, GSM cards and bank cards. Also, they are used as electronic passports and e-government cards such as personal identification and health care cards.

Basically a smart card consists of 3 main parts:

- Metallic unit on plastic material which is called plastic module (physical plastic card)
- Silicon chip located in the metallic unit on the plastic module. This chip consists of microprocessor, RAM, Non Volatile Memory and some hardware units
- Operating system (written in Non Volatile Memory and enables the operation of card functions using hardware units)

From the 3 parts listed above, only the third one is developed by TÜBİTAK-UEKAE. The first part is developed by a card manufacturer company (who provides the conditions that are presented in AKiS_TeslimveIsletim document) and the second part is developed by IFX Company. The second part has EAL 5+ (compatible with BSI0035) certificate. TOE operates on IFX SLE78CLFX1600PM chip. Chip consists of; 8051 based microprocessor, NVM, RAM, crypto co-processors, Random Number Generator, MMU, UART, Timers and MED.

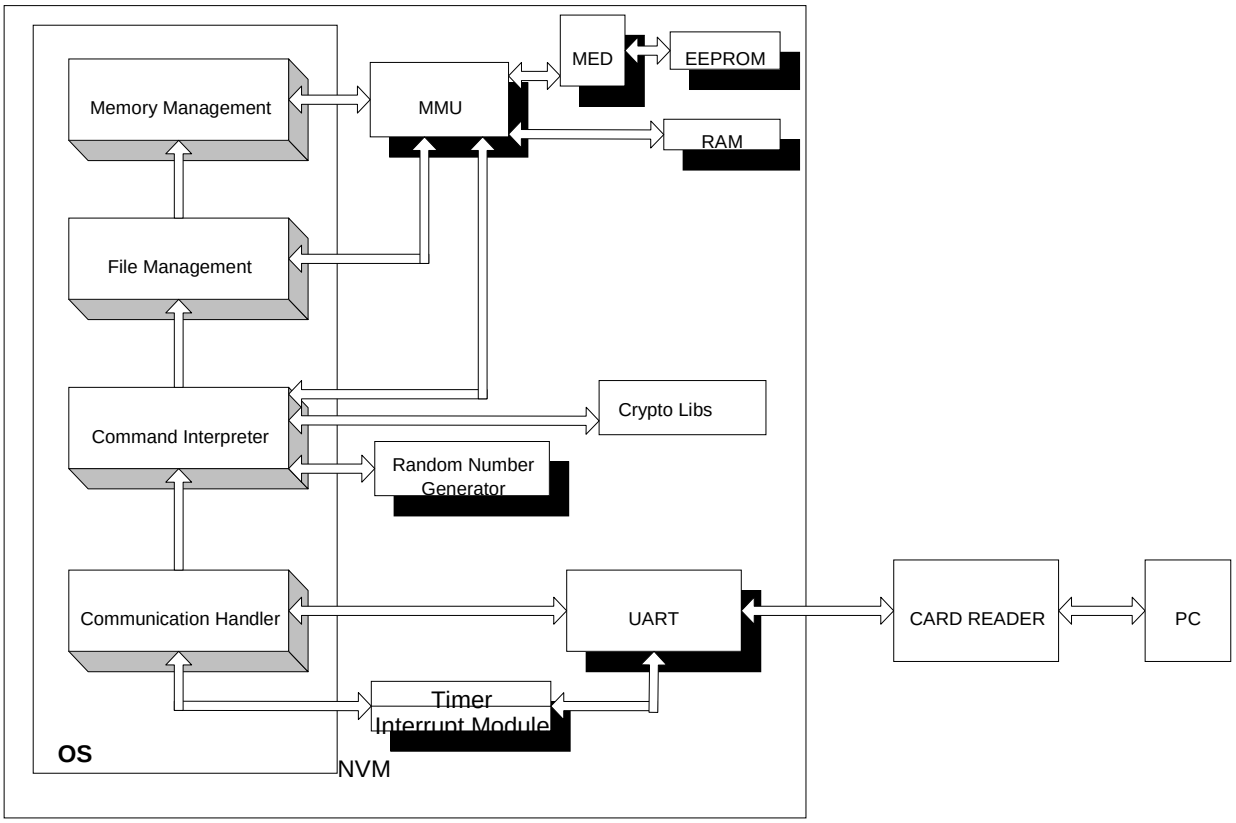
TOE is embedded in NVM during chip manufacturing and can't be changed afterwards. However, data can be written into EEPROM under operating system's control.

1.4.1.2.1 AKiS v1.4i Operating System Components

Operating system components are shown in Şekil 1;

- Memory Manager
- File Manager
- Command Interpreter
- Communication Handler

Message is received by UART which is managed by communication handler in TOE. The message comes in TPDU format which is mentioned above. Incoming TPDU packet is analysed and block type decision is made by the communication handler. TPDU may include 3 different types of blocks, named R, S and I block. R and S blocks are used to control the transmission protocol (ISO 7816-3). I block carries the command which is transmitted to the command interpreter and executed in TOE. When command execution is finished, communication handler sends the answer to the reader via UART. If the command is related with the file system, command interpreter calls the file manager. File manager is responsible for the operations in the file field which is in the EEPROM. Memory manager is used to open new file, close file, delete page and attach new page.



Şekil 1AKiS v1.4i Operating System components and environment

1.4.1.2.2 AKiS v1.4i Operating System Phases

AKiS v1.4i Operating System also consists of some phases which will be called as "AKiS v1.4i Operating System Life cycle phases" (Şekil 2) in order to obstruct a confusion.
There are 5 different life cycle phases available on TOE. Relations and crossing between these life cycle phases are shown in the Şekil 2. Also there are some several keys available on

TOE in order to be used within the execution of the secure commands. Command interpreter of TOE is designed to execute some special commands for the different life cycle phases.

These phases are;

Activation:

Main purposes of the activation phase is; to check if TOE is correct (not corrupted) and load the initial values of the keys that will be used on the execution of the secure commands (initialization and personalization key). MF (Master File) is created in this phase.

Initialization:

Main purpose of the initialization phase is to load the initialization data into the card. Therefore the file system will begin to construct on the EEPROM on each command.

Personalization:

Main purpose of the personalization phase is to load the personalization data into the card. Henceforth the card will include unique data belonging to the end user.

Operation:

In the operation phase, TOE is available for the end user.

Death:

When the security conditions listed below are not satisfied or it is noticed that security is trying to be surpassed, TOE enters the death phase:

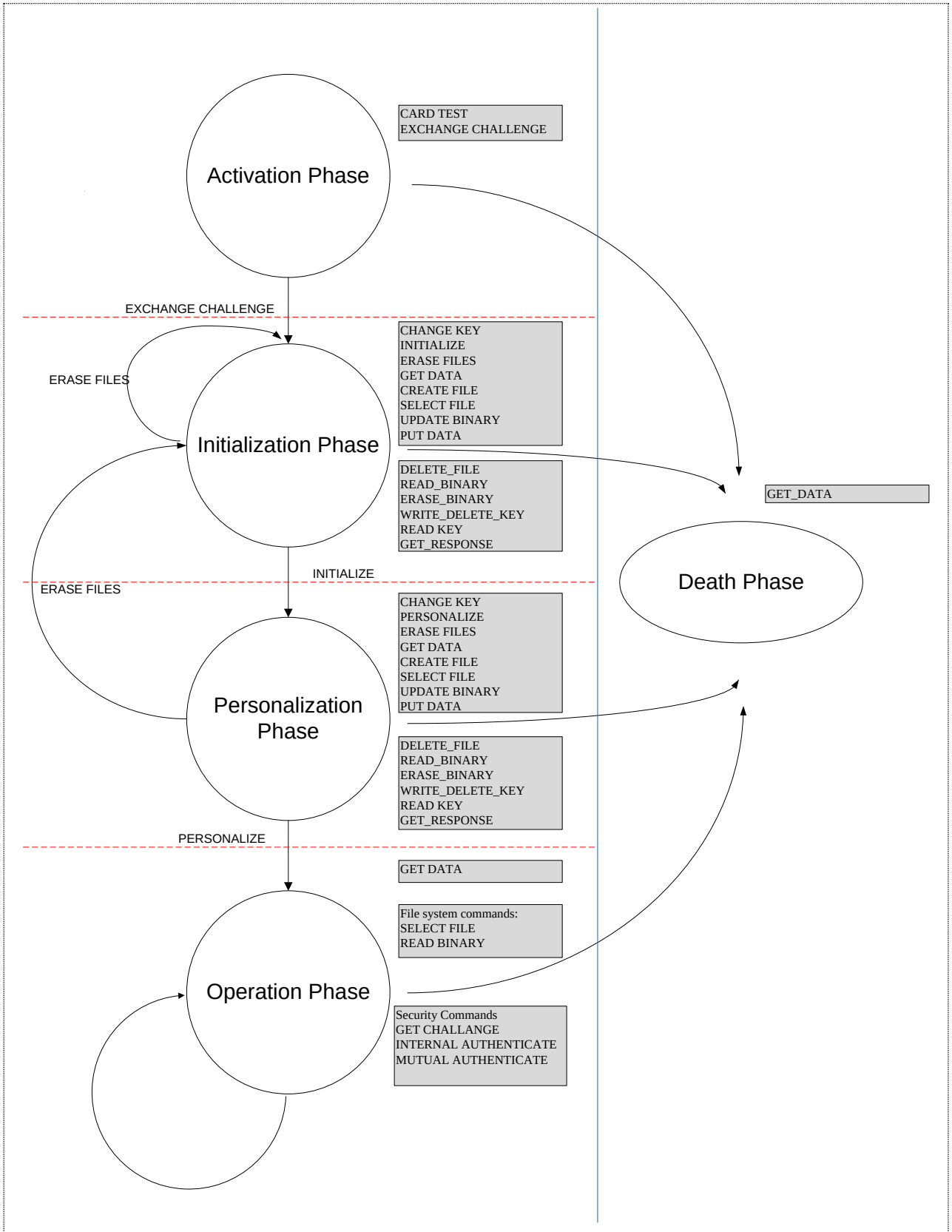
- When 64 unsuccessful authentication attempts occur related to loading of the system keys with Exchange Challenge command.
- When 10 unsuccessful authentication attempts occur related to changing of the initialization key with Change Key command, erasing of EEPROM with Erase Files command, Initialization Start and Initialization End commands.
- When 10 unsuccessful authentication attempts occur related tochanging of the personalization key with Change Key command, Personalization Start and Personalization End commands.
- When 16 to 128 (configurable) unsuccessful authentication attempts occur related to BAC authentication protocol.
- When an integrity check of interior filesystem tables fails.

1.4.1.3 The MRTD Application

The MRTD Application consists of LDS (Logical Data Structure), BAC(Basic Access Control) keys and active authentication keys.

1.4.1.4 The MRTD User Manual

Command set and operation of the AKiS Pasaport v1.4i operating system is described in this document.



Şekil 2AKiS-Pasaport OS Life Cycle Phases

1.4.2 Logical Scope of TOE

For this ST 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 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, EF.DG1),
(2) the digitized portraits (EF.DG2),
(3) the other data according to LDS (EF.DG5 to EF.DG16) and
(4) 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 organizational security measures (e.g. control of materials, personalization procedures). 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 sensitive biometrics as optional security measure in the 'ICAO Doc 9303'. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This ST addresses the protection of the logical MRTD
(i) in integrity by writeonly-once access control and by physical means, and
(ii) in confidentiality by the Basic Access Control Mechanism.
(iii) innon-clonability by the Active Authentication Mechanism.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system
(i) reads optically the MRTD,
(ii) authenticates itself as inspection system by means of Document Basic Access Keys.
After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system.

TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases, but TOE actually comprises of phase 1 and step 3 of phase 2.

Phase 1 "Development"

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The 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"

(Step3) 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 NVM The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step5) The MRTD manufacturer initializes the MRTD by these steps

(i) configuring the MRTD (choosing hash algorithm SHA-1 or SHA-256 for internal authenticate, enable attack counter, setting max BAC error number and delay, setting ATS historical bytes)
(ii) creating the MRTD application and
(iii) equiping MRTD's chips with pre-personalization Data.

Creation of the application implies the creation of MF and ICAO.DF

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"

(Step6) The personalization of the MRTD includes

(i) the survey of the MRTD holder's 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 of the TOE User Data and TSF Data into the logical MRTD and
(v) configuration of the TSF.

The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of

(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2), and
(iii) the Document security object.

The signing of the Document security object by the Document Signer 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.

The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise the Manufacturer Authentication Key, the Personalization Agent Authentication Key, the Basic Access Control Key, the Active Authentication Key, maximum value for attack counter and BAC error counter, active authentication hash algorithm type (SHA-1 or SHA-256 is chosen).

Phase 4 "Operational Use"
(Step7) The TOE is used as MRTD chip by the traveler and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

2 CONFORMANCE CLAIM

2.1 CC Conformance Claim

This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009, [2], Extended
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009, [3], Comformant

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [4]

has to be taken into account.

2.2 PP Claim

This ST claims conformance to Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control; BSI-CC-PP-0055, Version 1.10, 25th March 2009 [7].

2.3 Package Claim

EAL4 augmented with ALC_DVS.2.

2.4 Conformance Rationale

This ST claims strict conformance to the Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control; BSI-CC-PP-0055, Version 1.10, 25th March 2009. BSI-CC-PP-0055 is developed for ePassport applications with Basic Access Control according to ICAO 9303. The TOE referenced in this ST is same type of product with the TOE defined in the mentioned PP.

3 SECURITY PROBLEM DEFINITION

3.1 Introduction

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

The TOE specifies the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM

and Active Authentication mechanism.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4).

A sensitive 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 holder is used by the traveler to prove his possession of a genuine MRTD.

Subjects
This ST 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.

Personalization Agent
The agent is acting on behalf of the issuing State or Organization 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,

(iv) writing the initial TSF data and
(v) signing the Document Security Object.

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

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

The ***Basic Inspection System***(BIS)
(i) contains a terminal for the contactless 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 MRTD or other parts of the passport book providing this information.

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

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

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

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

3.2 Assumptions

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

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6
It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery MRTD delivery during steps 4 to 6
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

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

A.Pers_Agent 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 Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and
(iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object.

The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State

(i) examining an MRTD presented by the traveler and verifying its authenticity and
(ii) verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

(i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and
(ii) implements the terminal part of the Basic Access Control.

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

A.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

3.3 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

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

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

Asset: Anonymity of user,

T.Skimming Skimming the logical MRTD
Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE.
Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
Asset: confidentiality of logical MRTD data

T.Eavesdropping Eavesdropping to the communication between TOE and inspection system
Adverse action: An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.
Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance
Asset: confidentiality of logical MRTD data

T.Forgery Forgery of data on MRTD's chip
Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.
Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs
Asset: authenticity of logical MRTD data

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality
Adverse action: An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order
(i) to manipulate User Data,
(ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
(iii) to disclose or to manipulate TSF Data.
This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.
Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD
Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage Information Leakage from MRTD's chip

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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

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

Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper Physical Tampering

Adverse action: An attacker may perform physical probing of the MRTD's chip in order

(i) to disclose TSF Data or
(ii) to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

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

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified.

Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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

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

T.Malfunction Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

(i) deactivate or modify security features or functions of the TOE or
(ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing

administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.
Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD
Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

3.4 Organizational Security Policies

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

P.Manufact Manufacturing of the MRTD's chip
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.Personalization Personalization of the MRTD by issuing State or Organization only
The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by 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 (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys.

4 SECURITY OBJECTIVES

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

4.1 Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD
The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Documentsecurity object according to LDS and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

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

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

The traveler grants the authorization for reading the personal data inEF.DG1, EF.DG2 and EF.DG5 to EF.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. The Document Basic Access Keys are derivedfrom the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' that the inspectionsystem derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification Identification and Authentication of the TOE
The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC

during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 “Operational Use” the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

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 fortraceability 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. In the Phase 4 “Operational Use” the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

The following TOE security objectives address the protection provided by the MRTD’s chipindependent of the TOE environment.

OT.Prot_Abuse-Func Protection against Abuse of Functionality
After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to

(i) disclose critical User Data,
(ii) manipulate critical User Data of the IC Embedded Software,
(iii) manipulate Soft-coded ICEmbedded Software or
(iv) bypass, deactivate, change or explore security features or functions of the TOE.

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

OT.Prot_Inf_Leak 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.

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

- manipulation of the hardware and its security features, as well as controlled manipulation of memory contents (User Data, TSF Data) with a prior
- reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction Protection against Malfunctions
The TOE must ensure its correct operation. The TOE must prevent its operation outside thenormal 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.

A malfunction of the TOE may also be caused using a direct interactionwith elements on the chip surface. This is considered as being a manipulation (refer to theobjective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for the Operational Environment

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

OE.MRTD_Manufact Protection of the MRTD Manufacturing
Appropriate functionality testing of the TOE shall be used in step 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_ Delivery Protection of the MRTD delivery
Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process. Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

OE.Personalization Personalization of logical MRTD
The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization

(i) establish the correct identity of the holder and create biographical data for the MRTD,

(ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and

(iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The issuing State or Organization must

(i) generate a cryptographic secure Country Signing CA Key Pair,

(ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and

(iii) distribute the Certificate of the

Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must

(i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys,

(ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and

(iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG16 if stored in the LDS.

OE.BAC-Keys Cryptographic quality of Basic Access Control Keys

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

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

(i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

(ii) implements the terminal part of the Basic Access Control.

OE.Passive_Auth_Verif Verification by Passive Authentication

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

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

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x									x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										
T.Phys-Tamper							x									
T.Malfunction								x								
P.Manufact				x												
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							
A.MRTD_Delivery										x						
A.Pers_Agent											x					
A.Insp_Sys														x		x
A.BAC-Keys													x			

Table 2 - Security Objective Rationale

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

The OSP **P.Personalization**"Personalization of the MRTD by issuing State or Organization only" addresses the

(i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD", and

(ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers**"Access Control for Personalization of logical MRTD".

Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification**"Identification and Authentication of the TOE". The security objective **OT.AC_Pers**limits the management of TSF data and management of TSF to the Personalization Agent.

The OSP **P.Personal_Data**"Personal data protection policy" requires the TOE

(i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and

(ii) enforce the access control for reading as decided by the issuing State or Organization.

This policy is implemented by the security objectives **OT.Data_Int**"Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission.

The security objective **OT.Data_Conf**"Confidentiality of personal data" describes the protection of the confidentiality.

The threat **T.Chip_ID**"Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification**by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Skimming**"Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping "**Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf**"Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

The threat **T.Forgery**"Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers**"Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRTD passport book according to
OE.Exam_MRTD"Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign "**Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif**"Verification by Passive Authentication".

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

The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction**"Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak**"Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction**"Protection against Malfunctions". The assumption **A.MRTD_Manufact**"MRTD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_Manufact**"Protection of the MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

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

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

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys**"Inspection Systems for global interoperability" is covered by the security objectives for the TOEenvironment **OE.Exam_MRTD**"Examination of the MRTD passport book". The security
objectives for the TOE environment **OE.Prot_Logical_MRTD**"Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

5 EXTENDED COMPONENTS DEFINITION

This ST does not define extended components. The extended components defined in PP "Machine Readable Travel Document with „ICAO Application", Basic Access Control" are used and additionally FIA_API is added. These extended components are FAU_SAS, FCS_RND, FMT_LIM, FIA_API and FPT_EMSEC, and defined in the PP as given below.

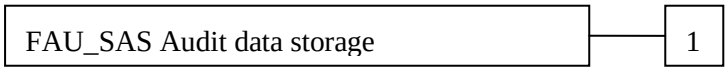
5.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements forthe storage of audit data. It has a more general approach than FAU_GEN, because it does notnecessarily require the data to be generated by the TOE itself and because it does not givespecific 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 behavior
This family defines functional requirements for the storage of audit data.

Component leveling



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

FAU_SAS.1 Audit storage

Hierarchical to: No other components.
Dependencies: No dependencies.

FAU_SAS.1-1 The TSF shall provide [assignment: *authorized users*] with the capabilityto store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functionalrequirements for random number generation used for cryptographic purposes. The componentFCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1.The similar component FIA_SOS.2 is intended for non-cryptographic use.

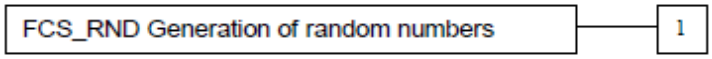
The family "Generation of random numbers (FCS_RND)" is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1-1 The TSF shall provide a mechanism to generate random numbers thatmeet [assignment: *a defined quality metric*].

5.3 Definition of the Family FIA_API

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

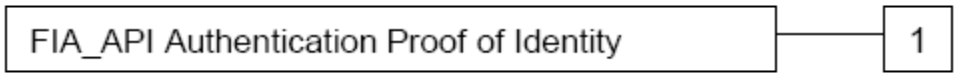
Application note 18: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behavior

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

Component leveling:



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.

Dependencies: No dependencies.

FIA_API.1-1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

5.4 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 themanagement of functions of the TSF. The examples of the technical mechanism used in the TOEshow that no other class is appropriate to address the specific issues of preventing the abuse offunctions by limiting the capabilities of the functions and by limiting their availability.

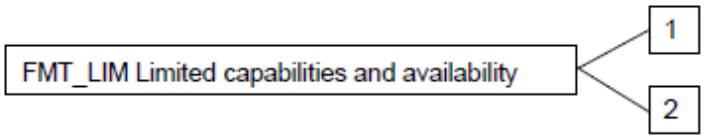
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

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

Component leveling:



FMT_LIM.1: Limited capabilities requires that the TSF is built to provide only thecapabilities (perform action, gather information) necessary for its genuinepurpose.

FMT_LIM.2: Limited availability requires that the TSF restrict the use of functions (referto 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 a sensitive family (FMT_LIM) ofthe Class FMT (Security Management) is defined here. This family describes the functionalrequirements for the Test Features of the TOE. The new functional requirements were defined inthe class FMT because this class addresses the management of functions of the TSF. Theexamples 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 thefunctions 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.
Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1-1 The TSF shall be designed in a manner that limits their capabilities sothat in conjunction with "Limited availability (FMT_LIM.2)" thefollowing policy is enforced [assignment: *Limited capability and availability policy*].

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

FMT_LIM.2 Limited availability
Hierarchical to: No other components.
Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2-1 The TSF shall be designed in a manner that limits their availability so thatin conjunction with "Limited capabilities (FMT_LIM.1)" the followingpolicy is enforced [assignment: *Limited capability and availability policy*].

The functional requirements FMT_LIM.1 and FMT_LIM.2 assume thatthere are two types of mechanisms (limited capabilities and limited availability) which togethershall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its userenvironment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with test and support functionality that is removed from,or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

5.5 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements forthe storage of audit data. It has a more general approach than FAU_GEN, because it does notnecessarily 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 behavior
This family defines functional requirements for the storage of audit data.

Component leveling

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.
Dependencies: No dependencies.

FAU_SAS.1-1 The TSF shall provide [assignment: authorized users] with the capability tostore [assignment: *list of auditinformation*] in theauditrecords.

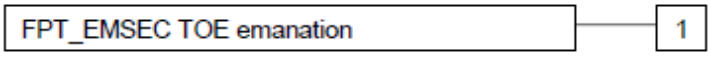
5.6 Definition of the Family FPT_EMSEC

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) isdefined here to describe the IT security functional requirements of the TOE. The TOE shallprevent attacks against the TOE and other secret data where the attack is based on externalobservable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE'selectromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA),timing attacks, etc. This family describes the functional requirements for the limitation ofintelligible emanations which are not directly addressed by any other component of CC part 2.

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

Family behavior
This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:
FPT_EMSEC.1-1:Limit of Emissions requires to not emit intelligible emissions enablingaccess to TSF data or user data.
FPT_EMSEC.1-2:Interface Emanation requires to not emit interface emanation enabling accessto 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.
Dependencies: No dependencies.

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 typesof 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 thefollowing interface [assignment: *type of connection*] to gain access to[assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 SECURITY REQUIREMENTS

6.1 Operation Notation for Functional Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration. Each ofthese operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in bold text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password.

The **iteration** operation is used when a component is repeated with varying operations. Iterated functional requirement components are shown with a "/**IDENTIFIER"** for the components which used more than once with varying operations.

6.2 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. The table below lists the SFRs that come from PP and that are out of PP.

SFRs from PP	**SFRs out of PP**
FAU_SAS.1	FCS_COP.1/SIGN
FCS_CKM.1	FIA_API.1
FCS_CKM.4	FIA_AFL.1/EXC
FCS_COP.1/SHA	FIA_AFL.1/INI
FCS_COP.1/ENC	FIA_AFL.1/PER
FCS_COP.1/AUTH	FMT_MTD.1/KEY_WRITE I2
FCS_COP.1/MAC	
FCS_RND.1	
FIA_UID.1	
FIA_AFL.1/BAC	
FIA_UAU.1	
FIA_UAU.4	
FIA_UAU.5	
FIA_UAU.6	
FDP_ACC.1	
FDP_ACF.1	
FDP_UCT.1	
FDP_UIT.1	
FMT_SMF.1	
FMT_SMR.1	
FMT_LIM.1	
FMT_LIM.2	
FMT_MTD.1/INI_ENA	

FMT_MTD.1/INI_DIS	
FMT_MTD.1/KEY_WRITE I1	
FMT_MTD.1/KEY_READ	
FPT_EMSEC.1	
FPT_TST.1	
FPT_FLS.1	
FPT_PHP.3	

Table 3- SFR List

6.2.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage
Hierarchical to: No other components.
Dependencies: No dependencies.

FAU_SAS.1-1 The TSF shall provide the *Manufacturer*[1] with the capability to store the *IC Identification Data*[2]in the audit records.

The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.2.2 Class FCS Cryptographic Support

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

FCS_CKM.1 Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1-1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:*Document Basic Access Key Derivation Algorithm*[3] and specified cryptographic key sizes *112 bit*[4] that meet the following: *[6],ICAO DOC 9303 normative appendix 5*[5].

[1][assignment: authorised users]
[2][assignment: list of audit information]
[3][assignment: cryptographic key generation algorithm]
[4][assignment: cryptographic key sizes]
[5][assignment: list of standards]

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 [6], normative appendix 5, A5.2, produces agreed parameters to generate the Triple- DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [6], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

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
Hierarchical to: No other components.
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.4-1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**card proprietary key access functions**] that meets the following: [***none***].

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

Refinement: Key destruction is performed via writing "00" to the key memory areas.

6.2.2.1 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/SHA Cryptographic operation – Hash for Key Derivation
Hierarchical to: No other components.
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

FCS_COP.1-1/SHA The TSF shall perform *hashing*[6]in accordance with a specifiedcryptographic algorithm *SHA-256*[7]and cryptographic key sizes *none*[8]that meet the following: *FIPS 180-2*[9].

[6][assignment: list of cryptographic operations]
[7][assignment: cryptographic algorithm]
[8][assignment: cryptographic key sizes]
[9][assignment: list of standards]

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) according to [6].

FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption Triple DES
Hierarchical to: No other components.
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

FCS_COP.1-1/ENC The TSF shall perform *secure messaging (BAC) – encryption anddecryption*[10]in accordance with a specified *cryptographic algorithm Triple-DES in CBC mode*[11] and *cryptographic key sizes 112 bit*[12] that meet the following: FIPS 46-3 [7] and [6]; normative appendix 5, A5.3[13].

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 and FIA_UAU.4.

FCS_COP.1/AUTH Cryptographic operation – Authentication
Hierarchical to: No other components.
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

FCS_COP.1-1/AUTH The TSF shall perform *symmetric authentication – encryption and decryption*[14] in accordance with a *specified cryptographic algorithm Triple-DES*[15] and *cryptographic key sizes 112 bit*[16]that meet the following: *FIPS 46-3* **[7]**[17].

This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC Cryptographic operation – Retail MAC
Hierarchical to: No other components.
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

[10][assignment: list of cryptographic operations]
[11][assignment: cryptographic algorithm]
[12][assignment: cryptographic key sizes]
[13][assignment: list of standards]
14[assignment: list of cryptographic operations]
15[assignment: cryptographic algorithm]
16[assignment: cryptographic key sizes]
17[assignment: list of standards]

FCS_COP.1-1/MAC The TSF shall perform *secure messaging – message authentication code*[18] in accordance with a *specified cryptographic algorithm Retail MAC*[19] and*cryptographic key sizes 112 bit*[20]that meet the following: *ISO 9797(MAC algorithm 3, block cipher DES, Sequence Message Counter,padding mode 2)*[21].

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 and FIA_UAU.4.

FCS_COP.1/SIGN Cryptographic operation – Signature Generation
Hierarchical to: No other components.
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

FCS_COP.1-1/SIGN The TSF shall perform signature generation[22] in accordance with a *specified cryptographic algorithm RSASSA-PSS*[23] and *cryptographic key sizes (1024 to 1848*[24]*) bit*that meet the following: *ISO/IEC 9796-2 scheme 1 and RFC 3447*[25].

6.2.2.2 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 Quality metric for random numbers
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RND.1-1 The TSF shall provide a mechanism to generate random numbers that meet *ANSI X9.17, AIS20 Class K4*[26].

This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

6.2.3 Class FIA Identification and Authentication

The Table 4 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [6], normative appendix 5, and [20]

18[assignment: list of cryptographic operations]
19[assignment: cryptographic algorithm]
20[assignment: cryptographic key sizes]
21[assignment: list of standards]
22[assignment: list of cryptographic operations]
23[assignment: cryptographic algorithm]
24[assignment: cryptographic key sizes]
25 [assignment: list of standards]
26[assignment: a defined quality metric].

Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES with 112 bit keys (cf. FCS_COP.1/AUTH)
Active Authentication Mechansim	FIA_API.1	RSASSA-PSS with 1024 to 1848 bit keys (FCS_COP.1/SIGN)

Table 4- Authentication mechanisms

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

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1-1 The TSF shall allow

1. *to read the Initialization Data in Phase 2 "Manufacturing",*
2. *to read the random identifier in Phase 3 "Personalization of the MRTD",*
3. *to read the random identifier in Phase 4 "Operational Use"*[27]

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.

The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. 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.

In the "Operational Use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier 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 a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specifiedbelow (Common Criteria Part 2).

[27][assignment: list of TSF-mediated actions]

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1-1 The TSF shall allow
1. *to read the Initialization Data in Phase 2 "Manufacturing",*
2. *to read the random identifier in Phase 3 "Personalization of the MRTD",*
3. *to read the random identifier in Phase 4 "Operational Use"*[28]

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.

The Basic Inspection System and the Personalization Agent authenticate themselves.

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

FIA_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4-1 The TSF shall prevent reuse of authentication data related to
1. Basic Access Control Authentication Mechanism,
2. Authentication Mechanism based on *Triple-DES*[29].

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [6]. In the first step the terminal authenticates itself 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 further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.5-1 The TSF shall provide
1. Basic Access Control Authentication Mechanism

[28][assignment: list of TSF-mediated actions]
[29][assignment: identified authentication mechanism(s)]

2. Symmetric Authentication Mechanism based on [selection: Triple-DES, AES] 28 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 Agentby one of the following mechanism(s)[selection: the Basic Access Control Authentication Mechanism withthe Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]],
2. the TOE accepts the authentication attempt as Basic InspectionSystem only by means of the Basic Access Control AuthenticationMechanism with the Document Basic Access Keys 29.

FIA_UAU.5/BAC Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.5-1/BAC The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. Symmetric Authentication Mechanism based on *Triple-DES*[30]

to support user authentication.

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

FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.6-1 The TSF shall re-authenticate the user under the conditions *each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism*[31].

The Basic Access Control Mechanism specified in [5] 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 for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

FIA_AFL.1/EXCAuthentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

[30][assignment: list of multiple authentication mechanisms]
[31][assignment: list of conditions under which re-authentication is required]

FIA_AFL.1-1/EXC The TSF shall detect when *[64]*[32] unsuccessful authentication attempts occur related to *loading of the system keys with Exchange Challenge command*[33].

FIA_AFL.1-2/EXC When the defined number of unsuccessful authentication attempts has been *met*[34], the TSF shall *force the card into death life cycle*[35].

FIA_AFL.1/INIAuthentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1-1/INI The TSF shall detect when *10*[36] unsuccessful authentication attempts occur related to *changing of the initialization key with Change Key command, erasing of EEPROM with Erase Files command, Initialization Start and Initialization End commands*[37].

Refinement: Change Key, Erase Files, Initialization Start and Initialization End commands use a common key counter which is updated in any unsuccessfull authentication attempt to any of these commands.

FIA_AFL.1-2/INI When the defined number of unsuccessful authentication attempts has been *met*[38], the TSF shall *force the card into death life cycle*[39].

FIA_AFL.1/PERAuthentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1-1/PER The TSF shall detect when *10*[40] unsuccessful authentication attempts occur related to *changing of the personalization key with Change Key command, Personalization Start and Personalization End commands*[41].

Refinement: Change Key, Personalization Start and Personalization End commands use a common key counter which is updated in any unsuccessfull authentication attempt to any of these commands.

FIA_AFL.1-2/PER When the defined number of unsuccessful authentication attempts has been *met*[42], the TSF shall *force the card into death life cycle*[43]**.**

[32][selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[33][assignment: list of authenticationevents]
[34][assignment: met or surpassed]
[35] [assignment: list of actions]
[36][selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[37][assignment: list of authentication events]
[38] [assignment: met or surpassed]
[39][assignment: list of actions]
[40][selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[41] [assignment: list of authentication events]
[42][assignment: met or surpassed]
[43] [assignment: list of actions]

FIA_AFL.1/BACAuthentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1-1/BAC The TSF shall detect when *an administrator configurable positive integer within [16 to 128]*[44] unsuccessful authentication attempts occur related to *BAC authentication protocol*[45].

FIA_AFL.1-2/BAC When the defined number of unsuccessful authentication attempts has been *met*[46], the TSF shall *wait for 2 to 10 seconds between the receiving the terminal challenge eIFD and sending the TSF response eICC during the BAC authentication attempts*[47].

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1-1 The TSF shall provide Active Authentication mechanism48 to prove the identity of the TOE49

Application Note: The TOE signs the challenge sent by the terminal with the Active Authentication Private Key and terminal verifies the identity of MRTD with the Chip Authentication Public Key.

6.2.4 Class FDP User Data Protection

6.2.4.1 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).

FDP_ACC.1 Subset access control – Basic Access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1-1 The TSF shall enforce the *Basic Access Control SFP*[50]on *terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD*[51].

[44] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[45][assignment: list of authentication events]
[46][assignment: met or surpassed]
[47][assignment: list of actions]
[48][assignment: *authentication mechanism*]
[49][assignment: *authorized user or role*
[50][assignment: access control SFP]
[51][assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

6.2.4.2 Security attribute 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).

FDP_ACF.1 Basic Security attribute based access control – Basic Access Control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1-1 The TSF shall enforce the *Basic Access Control SFP*[52]to objects based on the following:

1. *Subjects:*
   a. *Personalization Agent,*
   b. *Basic Inspection System,*
   c. *Terminal,*
2. *Objects:*
   a. *data EF.DG1 to EF.DG16 of the logical MRTD,*
   b. *data in EF.COM,*
   c. *data in EF.SOD,*
3. *Security attributes*
   a. *authentication status of terminals*[53].

FDP_ACF.1-2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,*
2. *the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD*[54].

FDP_ACF.1-3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[55].

FDP_ACF.1-4 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. *Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.*
2. *Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.*
3. *The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4*[56].

[52][assignment: access control SFP]
[53][assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes]
[54][assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[55][assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[56][assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

6.2.4.3 Inter-TSF-Transfer

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

FDP_UCT.1 Basic data exchange confidentiality - MRTD
Hierarchical to: No other components.
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_UCT.1-1 The TSF shall enforce the *Basic Access Control SFP*[57] to be able to transmit and *receive*[58] user data in a manner protected from unauthorised disclosure.

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

FDP_UIT.1 Data exchange integrity - MRTD
Hierarchical to: No other components.
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_UIT.1-1 The TSF shall enforce the *Basic Access Control SFP*[59] to be able to *transmit and receive*[60]user data in a manner protected from *modification, deletion, insertion and replay*[61]errors.

FDP_UIT.1-2 The TSF shall be able to determine on receipt of user data, *whether modification, deletion, insertion and replay*[62] has occurred.

6.2.5 Class FMT Security Management

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

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1-1 The TSF shall be capable of performing the following management functions:
1. *Initialization,*
2. *Pre-personalization,*
3. *Personalization*[63].

[57][assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[58][selection*: transmit, receive*]
[59][assignment: access control SFP(s) and/or information flow control SFP(s)
[60][selection: transmit, receive]
[61][selection: modification, deletion, insertion, replay]
[62][selection: modification, deletion, insertion, replay]

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

FMT_SMR.1 Security roles
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1-1 The TSF shall maintain the roles
1. *Manufacturer,*
2. *Personalization Agent,*
3. *Basic Inspection System*[64].

FMT_SMR.1-2 The TSF shall be able to associate users with roles
The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below(Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities
Hierarchical to: No other components.
Dependencies: FMT_LIM.2 Limited availability.

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*[65]

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

FMT_LIM.2 Limited availability
Hierarchical to: No other components.
Dependencies: FMT_LIM.1 Limited capabilities.

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*[66].

---

[63][assignment: list of management functions to be provided by the TSF]
[64][assignment: theauthorisedidentifiedroles]
[65] [assignment: Limited capability and availability policy]
[66][assignment: Limited capability and availability policy]

The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

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

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Prepersonalization Data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1-1/INI_ENA The TSF shall restrict the ability to *write*[67]*the Initialization Data and Prepersonalization Data*[68]to *the Manufacturer*[69].

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 Key.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1-1/INI_DIS The TSF shall restrict the ability to *disable read access for users* to[70] theInitialization Data[71] to the Personalization Agent[72].

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 Prepersonalization 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 a 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.

[67][selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[68][assignment: list of TSF data]
[69][assignment: the authorised identified roles]
[70][selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[71][assignment: list of TSF data]
[72][assignment: the authorised identified roles]

FMT_MTD.1/KEY_WRITE I1 Management of TSF data – Key Write Initialization 1
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_WRITEI1 The TSF shall restrict the ability to *write*[73] the *Document Basic Access Keys*[74]to the *Personalization Agent*[75].

FMT_MTD.1/KEY_WRITE I2 Management of TSF data – Key Write Initialization 2
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_WRITE I2 The TSF shall restrict the ability to *write*[76]*the Active Authentication Keys*[77] to the *Personalization Agent*[78].

FMT_MTD.1/KEY_READ Management of TSF data – Key Read
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1-1/KEY_READ
The TSF shall restrict the ability to *read*[79]the *Document Basic Access Keys and Personalization Agent Keys*[80] to *none*[81].

The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.2.6 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 SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

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

---

[73][selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[74][assignment: list of TSF data]
[75][assignment: list of TSF data]
[76][selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[77] [assignment: list of TSF data]
[78][assignment: the authorised identified roles]
[79][selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[80][assignment: list of TSF data]
[81][assignment: the authorised identified roles]

FPT_EMSEC.1 TOE Emanation
Hierarchical to: No other components.
Dependencies: No Dependencies.

FPT_EMSEC.1-1 The TOE shall not emit *power variations, timing variations during command execution*[82] in excess of *non-useful information*[83] enabling access to *Personalization Agent Key(s)*[84] and *none*[85].

FPT_EMSEC.1-2 The TSF shall ensure *any unauthorized users*[86] are unable to use the *following interface smart card circuitcontacts*[87] to gain access to *Personalization Agent Key(s)*[88] and *none*[89].

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

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

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No Dependencies.

FPT_FLS.1-1 The TSF shall preserve a secure state when the following types of failures occur:
1. *Exposure to out-of-range operating conditions where therefore a malfunction could occur,*
2. *failure detected by TSF according to FPT_TST.1*[90].

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

FPT_TST.1 TSF testing
Hierarchical to: No other components.
Dependencies: No Dependencies.

FPT_TST.1-1 The TSF shall run a suite of self tests *at the conditions [during initial startup, when any command is received, during cryptographic operations]*[91] to demonstrate the correct operation of *the TSF*[92].
FPT_TST.1-2 The TSF shall provide authorised users with the capability to verify the

---

[82][assignment: types of emissions]
[83][assignment: specified limits]
[84][assignment: list of types of TSF data]
[85][assignment: list of types of user data]
[86][assignment: type of users]
[87][assignment: type of connection]
[88][assignment: list of types of user data]
[89][assignment: list of types of user data]
[90][assignment: list of types of failures in the TSF]
[91] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]
[92][selection: [assignment: parts of TSF], the TSF]

integrity of *TSF data*[93].
FPT_TST.1-3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

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

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_PHP.3-1 The TSF shall resist *physical manipulation and physical probing*[94] to *the TSF*[95] by responding automatically such that the SFRs are always enforced.

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 SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.3 Security Assurance Requirements for the TOE

The 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 component: ALC_DVS.2.

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

[93][selection: [assignment: parts of TSF], TSF data]
[94][assignment: physical tampering scenarios]
[95][assignment: list of TSF devices/elements]

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_COP.1/SIGN		x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1/EXC			x					
FIA_AFL.1/INI	x		x					
FIA_AFL.1/PER	x		x					
FIA_AFL.1/BAC			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					
FIA_UAU.5	x	x	x					
FIA_UAU.6	x	x	x					
FIA_API.1				x				
FDP_ACC.1	x	x	x					
FDP_ACF.1	x	x	x					
FDP_UCT.1	x	x	x					
FDP_UIT.1	x	x	x					
FMT_SMF.1	x	x	x					
FMT_SMR.1	x	x	x					
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA				x				
FMT_MTD.1/INI_DIS				x				
FMT_MTD.1/KEY_WRITE I1, I2	x	x	x					
FMT_MTD.1/KEY_READ	x	x	x					
FPT_EMSEC.1	x				x			
FPT_TST.1					x		x	
FPT_FLS.1	x				x		x	
FPT_PHP.3	x				x	x		

Table 5- Coverage of Security Objective for the TOE by SFR

The security objective **OT.AC_Pers**"Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/ AUTH).

FIA_AFL.1/INI and FIA_AFL.1/PER describe the authentication failures and the actions taken after unsuccessfull authentication attempts during initialization and personalization.

In case of using the BAC mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int**"Integrity of personal data" requires the TOE to protect the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int**"Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the BAC mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ. FCS_COP.1/SIGN requires the protection of the integrity of the logical MRTD data by active authentication mechanism.

The security objective **OT.Data_Conf**"Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys). FCS_COP.1/SIGN requires the protection of confidentiality of the logical MRTD data by active authentication mechanism. FIA_AFL.1/EXC, FIA_AFL.1/BAC, FIA_AFL.1/INI and FIA_AFL.1/PER prevent unauthenticated users to access logical MRTD data.

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. The SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/ MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document Basic Access Keys.

Note, neither the security objective OT.Data_Conf nor the SFR FIA_UAU.5 requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

The security objective **OT.Identification**"Identification and Authentication of the TOE" address the storage of the IC Identification Data uniquely identifying the MRTD's chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1. Furthermore, the TOE shall identify itself only to a successful authenticated Basic InspectionSystem in Phase 4 "Operational Use". The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD's chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts related to BAC authentication protocol, FIA_AFL.1/BAC enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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

The security objective **OT.Prot_Inf_Leak**"Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure
- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

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

The security objective **OT.Prot_Malfunction**"Protection against Malfunctions" is covered by

(i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and

(ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.4.2 Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

The table 4 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of theDependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographickeydistributionor FCS_COP.1 Cryptographicoperation], FCS_CKM.4 Cryptographickeydestruction,	Fulfilledby FCS_COP.1/ENC and FCS_COP.1/MAC, Fulfilledby FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of userdatawithoutsecurityattributes, FDP_ITC.2 Import of user data withsecurityattributes, or FCS_CKM.1 Cryptographickeygeneration]	Fulfilledby FCS_CKM.1,
FCS_COP.1/SHA	[FDP_ITC.1 Import of userdatawithoutsecurityattributes, FDP_ITC.2 Import of user data withsecurityattributes, or FCS_CKM.1 Cryptographickeygeneration], FCS_CKM.4 Cryptographickeydestruction	justification 1 fornon-satisfieddependencies, Fulfilledby FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of userdatawithoutsecurityattributes, FDP_ITC.2 Import of user data withsecurityattributes, or FCS_CKM.1 Cryptographickeygeneration], FCS_CKM.4 Cryptographickeydestruction	Fulfilledby FCS_CKM.1, Fulfilledby FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of userdatawithoutsecurityattributes, FDP_ITC.2 Import of user data withsecurityattributes, or FCS_CKM.1 Cryptographickeygeneration], FCS_CKM.4 Cryptographickeydestruction	justification 2 fornon-satisfieddependenciesjustification 2 fornon-satisfieddependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of userdatawithoutsecurityattributes, FDP_ITC.2 Import of user data withsecurityattributes, or FCS_CKM.1 Cryptographickeygeneration], FCS_CKM.4 Cryptographickeydestruction	Fulfilledby FCS_CKM.1, Fulfilledby FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1 /BAC	FIA_UAU.1 Timing of authentication	Fulfilledby FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilledby FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.

FDP_ACC.1	FDP_ACF.1 Security attributebasedaccesscontrol	Fulfilledby FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subsetaccesscontrol, FMT_MSA.3 Staticattributeinitialization	Fulfilledby FDP_ACC.1, justification 3 fornon-satisfieddependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trustedchannel, or FTP_TRP.1 Trustedpath], [FDP_IFC.1 Subsetinformationflowcontrolor FDP_ACC.1 Subsetaccesscontrol]	justification 4 fornon-satisfieddependenciesFulfilledby FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trustedchannel, or FTP_TRP.1 Trustedpath], [FDP_IFC.1 Subsetinformationflowcontrolor FDP_ACC.1 Subsetaccesscontrol]	justification 4 fornon-satisfieddependenciesFulfilledby FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilledby FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilledby FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilledby FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of managementfunctions, FMT_SMR.1 Security roles	Fulfilledby FMT_SMF.1 Fulfilledby FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of managementfunctions, FMT_SMR.1 Security roles	Fulfilledby FMT_SMF.1 Fulfilledby FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of managementfunctions, FMT_SMR.1 Security roles	Fulfilledby FMT_SMF.1 Fulfilledby FMT_SMR.1
FMT_MTD.1/KEY_WRITE I1, I2	FMT_SMF.1 Specification of managementfunctions, FMT_SMR.1 Security roles	Fulfilledby FMT_SMF.1 Fulfilledby FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 6 – Dependencies between the SFR for the TOE

Justification for non-satisfied dependencies between the SFR for TOE:
No. 1: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.
No. 2: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.
No. 3: The access control TSF according to FDP_ACF.1 uses security attributes which are

defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
No. 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.4.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security Requirements

Dependencies ALC_DVS.2: no dependencies.

6.4.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:
The dependency analysis in Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not

to arise in Dependency Rationale and Security Assurance Requirements Rationale. Furthermore, as also discussed in Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in Dependency Rationale and Security Assurance Requirements Rationale. Furthermore, as also discussed in Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification

7.1 TOE Security Functions

7.1.1 Cryptographic Operations

This function implements the following cryptographic operations for the TOE:

1. 3DES key generation according to Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit.
2. Hashing according to SHA-1 and SHA-256 that meets FIPS 180-2. For Basic Access Control SHA-1 is used. For active authentication manufacturer decides which algorithms will be used : SHA-1 or SHA-256.
3. Secure messaging: encryption and decryption with 3DES algorithm in CBC mode with key sizes of 112 bits. 8 bytes zero IV, padding mode 2 is used.
4. Secure messaging: message authentication with Retail MAC with key sizes 112 bits according to ISO 9797. MAC Algorithm 3 is used with block cipher 3DES.
5. Active authentication signature generation according to ISO/IEC 9796-2 scheme 1 with RSA algorithm RFC 3447 RSASSA-PSS key sizes 1024 to 1848 bits.
6. After each active authentication, active authentication keys are destroyed by writing 0.
7. After each BAC session both the 3DES encryption key and message authentication key are destroyed by writing 0.
8. After each initialization authentication and personalization authentication, initialization key and personalization key are destroyed by writing 0.
9. Random number generation according to ANSI X9.17, AIS20 Class K4 for key generation, authentication operations.

7.1.2 Identification and Authentication

This function implements the following identification and authentication operations for the TOE:

1. Storage of IC Identification data by the Manufacturer (with PUT DATA command)
2. The following data can be read before identification and authentication
    a. Initialization data in Manufacturing phase
    b. ATS (Answer to Select) in all phases
3. TSF mediated actions require successful identification and authentication, because BAC is activated.

4. Authentication data (random numbers) are prevented to be reused.
5. User authentication is provided through:
    a. BAC authentication mechanism in Operation Phase through BAC Authenticaton mechanism with Document Basic Access keys.
    b. Symmetric authentication mechanism based on 3DES in Manufacturing Phase with initialization key.
    c. Symmetric authentication mechanism based on 3DES in Personalization Phase with personalization key.
6. Active authentication of the TOE is provided through Active authentication mechanism with active authentication keys.

7.1.3 User Data Protection

This function implements the following user data protection operations for the TOE:

1. Allowing only the successfully authenticated Personalization Agent to read and write EF.SOD, EF.COM anddata groups DG1 to DG16 of the LDS.
2. Allowing the terminals to read data groups DG1-DG2 andDG5 to DG 16 of the LDS after successful BAC authentication.
3. Not allowing anybody to modify any data groups DG1 to DG 16 of the LDS in Operation phase.
4. Not allowing anybody to write/modify/erase any data (keys, LDS data) in Operation phase.
5. Transmitted and received user data is protected from modification, deletion, insertion and replay errors through secure messaging.
6. Determination on receipt of user data if modification, deletion, insertion and replay have occurred through secure messaging.
7. Not allowing anybody to read DG3 and DG4.

7.1.4 Security Management

This function implements the following security management operations for the TOE:

1. Initialization, personalization and configuration of the TOE are only allowed for the manufacturer and the personalization agent.
2. Initialization data and pre-personalization data can only be written by the manufacturer.
3. Ability to set maximum value of the BAC error counter and wait time for the BAC error is restricted to the manufacturer.
4. When BAC error counter exceeds the threshold, the TOE waits for a pre-configured wait time without any action.
5. Ability to set the hash algorithm for the active authentication, SHA-1 or SHA-256, is restricted to the manufacturer and the personalization agent.
6. Maintenance of the security roles: Manufacturer, personalization agent, Basic Inspection System.
7. Personalization Agent is allowed to write the Document Basic Access Keys.
8. Manufacturer and Personalization Agent are allowed to write the Active Authentication keys.

9. After unsuccessfull authentication in INITIALIZATION START, INITIALIZATION END, and CHANGE KEY commands in Manufacturing phase, the initialization key error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used.
10. After unsuccessfull authentication in PERSONALIZATION START, PERSONALIZATION END, CHANGE KEY commands in Personalization phase, the personalization key error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used.
11. After unsuccessfull authentication in EXCHANGE CHALLENGE command in Manufacturing phase, the EXCHANGE CHALLENGE error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used which may enable other attacks.
12. Nobody is allowed to read Document Basic Access keys and Active Authentication Private keys.
13. Test features of the TOE are not available in Operation phase. If test features are performed by the TOE, no user data, TSF data can be disclosed or manipulated, no software can be reconstructed and no substantial information about TSF can be gathered.
14. Ability to disable read access for users to theInitialization Data to the Personalization Agent.

7.1.5 Protection

This function protects the TSF, TSF data and user data. It implements the following protection operations for the TOE:

1. Masking in the core supports the protection of data transfers and calculations. It is important to realize a random timing behavior for code execution so that the same code will always produce a different timing profile. Random Timing Jitter is a useful tool against different form of side-channel attacks.
2. The cache is a vital component of the SLE 78 family and contributes significantly to the processor performance. PFD (Post Failure Detection) cache integrity check to detect distinct memory manipulation.
3. Security Trap Handling on User Mode Security Live Control allows “emergency” handling to be carried out in the case of a security alarm. UmSLC Test tests sensors and alarms.
4. Watchdog supports detection of program flow manipulations. It can be combined with checkpoint functionality.
5. Level Concept satisfies hierchical separation of code blocks with different access rights and restricted code access for unprivileged levels..
6. FixKey is general IP protection. VarKey is specific temporarily required secrets. MED-Configuration of Rounds protect of highly sensitive data.
7. One of Random Number Generators is True Random Number Generator. It provides highest quality true random numbers for any kind of cryptographic seed. No online test is required. Other Random Number Generator is Pseudo Random Number Generator (PRNG). It is used for high performance random number generation.
8. Symmetric Crypto Processor (SCP) is coprocessor for fully built-in triple-DES and AES with keys up to 256 bits. Crypto engine (Crypto@2304T) for public key Cryptography satisfies RSA with register lengths of up to 2304 bits, RSA calculations with key lengths of up to: 2048 bits w/o CRT and 4096 bits with CRT.

9. TSF Data integrity check, tests the TSF data before usage and if any manipulation is detected the TOE enters Death phase.
10. TSF code integrity check allows the authorized user to check the integrity of the TSF Code.

In this section it is shown that security functions fulfill security requirements. At least one security function meets each security requirement. The numbers indicate the operation number listed under the security functions chapter.

	Cryptographic Operation	Identification and Authentication	User Data Protection	Security Management	Protection
FAU_SAS.1-1		1			
FCS_CKM.1-1	1				
FCS_CKM.4-1	6,7,8				
FCS_COP.1-1/SHA	2			5	
FCS_COP.1-1/ENC	3				
FCS_COP.1-1/AUTH	3				
FCS_COP.1-1/MAC	4				
FCS_COP.1-1/SIGN	5				
FCS_RND.1-1	9				7
FIA_UID.1-1		2			
FIA_UID.1-2		3			
FIA_UAU.1-1		2			
FIA_UAU.1-2		3			
FIA_UAU.4-1		4			
FIA_UAU.5-1		5			
FIA_UAU.5-2		5			
FIA_UAU.6-1		5			
FIA_API.1-1	5	6			
FIA_AFL.1-1/EXC				11	
FIA_AFL.1-2/EXC				11	
FIA_AFL.1-1/INI				9,	
FIA_AFL.1-2/INI				9,	
FIA_AFL.1-1/PER				10,	
FIA_AFL.1-2/PER				10,	
FIA_AFL.1-1/BAC				3	
FIA_AFL.1-2/BAC				4	
FDP_ACC.1-1			1		

FDP_ACF.1-1			2		
FDP_ACF.1-2			1,2,7		
FDP_ACF.1-3			1,2		
FDP_ACF.1-4			3,4		
FDP_UCT.1-1			5		
FDP_UIT.1-1			5		
FDP_UIT.1-2			6		
FMT_SMF.1-1				1	
FMT_SMR.1-1				6	
FMT_SMR.1-2				6	
FMT_LIM.1-1				13	
FMT_LIM.2-1				13	
FMT_MTD.1-1/INI_ENA				2	
FMT_MTD.1-1/INI_DIS				14	
FMT_MTD.1-1/KEY_WRITE I1,I2				7,8	
FMT_MTD.1-1/KEY_READ				12	
FPT_EMSEC.1-1					1,6,8
FPT_EMSEC.1-2					1,6,8
FPT_FLS.1-1					2
FPT_TST.1-1					3
FPT_TST.1-2					9
FPT_TST.1-3					10
FPT_PHP.3-1					2,4,5

Table 7 - Summary specification rationale table

8 Statement of Compatibility between the Composite Security Target and the Platform Security Target

This chapter shows that the security objectives, security requirements and security functionality in the Composite-ST and the Platform-ST are compatible.

8.1 Separation of the Platform-TSF

Security functions for the platform and their usage in TOE are listed below. They are categorized as "relevant Platform-TSF" if TOE uses this TSF and "irrelevant Platform-TSF" if they are not used.

Relevant Platform Security Functionality	Irrelevant Platform Security Functionality
SF_PS Protection against Snooping	SF_DPM Device Phase Management
SF_PMA Protection against Modification Attacks	SF_PLA Protection against Logical Attacks
SF_CS Cryptographic Support	

8.1.1 Relevant Platform Security Functionality

SF_PS Protection against Snooping

This function is relevant Platform-TSF, TOE is protected against snooping. All contents of memories of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data.

SF_PMA Protection against Modification Attacks

This function is relevant Platform-TSF, because the TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and result comparison of all tasks to detect incorrect calculations. The detection of an incorrect calculation is stored and the TOE enters a defined secure state which causes the chip internal reset process. Whenever a physical manipulation or a physical probing attack is detected, the processing of the TOE is immediately stopped and the TOE enters a secure state called security reset.

SF_CS Cryptographic Support

This function is relevant Platform-TSF, because the TOE uses Triple DES coprocessor in Triple DES operations (encryption/decryption), RSA coprocessor in RSA operations(Encryption, Decryption, Signature Generation and Verification) and the SHA-2 library for hash value calculation. Additionally, Toolbox Library , Base Library and TRNG is used by TOE. Toolbox Library provides the basic long integer arithmetic and modular functions in software, supported by the crytographic coprocessor. Base Library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface. The TOE is equipped with physical True Random Number Generator(TRNG).

8.1.2 Irrelevant Platform Security Functionality

SF_DPM Device Phase Management

This function is irrelevant.

SF_PLA Protection against Logical Attacks

This function is non-relevant Platform-TSF , because the TOE does not use privilege levels of the CPU and memory access controls offered by the platform.

8.2 Platform-SFR

Platform SFR	Composite SFR	Rational
FRU_FLT.2 Limited fault tolerance	• FPT_EMSEC.1 TOE Emanation • FPT_PHP.3 Resistance to physical attack	Platform SFR FRU_FLT.2 is used to support following Composite SFRs: • FPT_EMSEC.1 TOE Emanation and • FPT_PHP.3 Resistance to physical attack
FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1 Failure with preservation of secure state	The requirements match they have the same meaning
FMT_LIM.1 Limited capabilities	FMT_LIM.1 Limited capabilities	The requirements match they have the same meaning
FMT_LIM.2 Limited availability	FMT_LIM.2 Limited availability	The requirements match they have the same meaning
FAU_SAS.1 Audit storage	FAU_SAS.1Audit storage	The requirements match they have the same meaning
FPT_PHP.3 Resistance to physical attack	FPT_PHP.3 Resistance to physical attack	The requirements match they have the same meaning
FDP_ITT.1 Basic internal transfer protection	• FPT_EMSEC.1 TOE Emanation • FPT_PHP.3 Resistance to physical attack	Platform SFR FRU_FLT.2 is used to support following Composite SFRs: • FPT_EMSEC.1 TOE Emanation and • FPT_PHP.3 Resistance to physical attack
FPT_ITT.1 Basic internal TSF data transfer protection	• FPT_EMSEC.1 TOE Emanation • FPT_PHP.3 Resistance to physical attack	Platform SFR FRU_FLT.2 is used to support following Composite SFRs: • FPT_EMSEC.1 TOE Emanation and • FPT_PHP.3 Resistance to physical attack
FDP_IFC.1 Subset information flow control	• FPT_EMSEC.1 TOE Emanation • FPT_PHP.3 Resistance to physical attack	Platform SFR FRU_FLT.2 is used to support following Composite SFRs: • FPT_EMSEC.1 TOE Emanation and • FPT_PHP.3 Resistance to physical attack
FCS_RNG.1 Quality metric for random numbers	FCS_RND.1	The requirements match they have the same meaning
FPT_TST.2 Subset TOE security testing	FPT_TST.1.1 TSF testing	Composite product runs the self tests provided by platform.
FDP_ACC.1 Subset access control		Not used by composite product.
FDP_ACF.1 Security attribute based		Not used by composite product.

access control		
FMT_MSA.1 Management of security attributes		Not used by composite product.
FMT_MSA.3 Static attribute initialization		Not used by composite product.
FMT_SMF.1 Specification of Management functions		Not used by composite product.
FCS_CKM.1 Cryptographic key management		Not used by composite product.
FDP_SDI.1 Stored data integrity monitoring		Supports the composite SFR :FPT_PHP.3 Resistance to physical attack
FDP_SDI.2 Stored data integrity monitoring and action		Supports the composite SFR :FPT_PHP.3 Resistance to physical attack
FCS_COP.1 [DES]	FCS_COP.1/ENC	The requirements match they have the same meaning
FCS_COP.1 [AES]		This SFR of the platform is not used by the TOE.
FCS_COP.1 [RSA]		Supports the composite SFR, FIA_API.1
FCS_COP.1[ECDSA]		This SFR of the platform is not used by the TOE.
FCS_COP.1 [ECDH]		This SFR of the platform is not used by the TOE.
FCS_COP.1 [SHA]	FCS_COP.1/SHA	The requirements match they have the same meaning

Table 8 - Security requirements mapping table

8.3 Platform Security Objectives

Platform Security Objective	Composite Security Objective	Rationale
O.Leak-Inherent	OT.Prot_Inf_Leak	The security objectives match
O.Mem_Access		This objective is not related
O.Phys-Probing	OT.Prot_Phys-Tamper	The security objectives match
O.Malfunction	OT.Prot_Malfunction	The security objectives match
O.Phys-Manipulation	OT.Data_Int OT.Prot_Phys-Tamper	The security objectives match
O.Leak-Forced	OT.Prot_Inf_Leak	The security objectives match
O.Abuse-Func	OT.Prot_Abuse-Func	The security objectives match
O.Identification	OT.Identification	The security objectives match
O.RND		This is used by embedded OS according to FCS_RND.1
O.Add-Functions		Additional functions are Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES),

		Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (EC), Secure Hash Algorithm (SHA-2). Besides EC, they are used by embedded OS.

Table 9 - Security objectives mapping table

8.4 Platform Security Objectives for the environment

Platform Security Objective	Composite Security Objective	Rationale
OE.Plat-Appl	OT.Prot_Inf_Leak	The security objectives match
OE.Resp-Appl	OT.AC_Pers, OT.Data_Int, OT.Data_Conf	The security objectives match
OE.Process-Sec-IC	OE.MRTD_Manufact	The security objectives match

Table 10 - Security objectives for the environment mapping table

8.5 Platform-Assumptions

Platform Assumptions	Composite Assumptions	Rationale
A.Process-Sec-IC	A.MRTD_Delivery A.Pers_Agent	Covered by A.MRTD_Delivery, A.Pers_Agent assumptions and ALC SAR class of composite product.
A.Plat-Appl		Considered for the development of the embedded OS
A.Resp-Appl		Considered for the development of the embedded OS
A.Key-Function		Considered for the development of the embedded OS

Table 11 - Assumptions mapping table

8.6 Platform-OSPs

Platform OSP	Composite OSP	Rationale
P.Process-TOE	P.Manufact P.Personalization	The OSPs match
P.Add-Functions		This policy supports Cryptographic Support SFRs.

Table 12 - OSP mapping table

8.7 Platform-Threats

Platform Threats	Composite Threats	Rationale
T.Leak-Inherent	T.Information_Leakage	The threats match
T.Phys-Probing	T.Phys-Tamper	The threats match
T.Malfunction	T.Malfunction	The threats match
T.Phys-Manipulation	T.Forgery T.Phys-Tamper	The threats match
T.Leak-Forced	T.Information_Leakage, T.Phys-Tamper, T.Malfunction	The threats match
T.Abuse-Func	T.Abuse-Func	The threats match
T.Mem-Access		The threat is not specified in composite ST
T.RND		The threat is not specified in composite ST, however it is used by the composite ST.

Table 13 - Threats mapping table

9 REFERENCES

CommonCriteria

[1] CommonCriteriafor Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] CommonCriteriafor Information Technology Security Evaluation, Part 2: Security FunctionalComponents; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] CommonCriteriafor Information Technology Security Evaluation, Part 3: Security AssuranceRequirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] CommonMethodologyfor Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version3.1, Revision 3, July 2009

ICAO

[5]ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine ReadablePassports,Sixth Edition, 2006, International CivilAviationOrganization

[6]Machine Readable Travel Document with „ICAO Application", Basic Access Control; BSI-CC-PP-0055, Version 1.10, 25th March 2009, BundesamtfürSicherheit in der Informationstechnik

[7] Security TargetM7820 M11includingoptional Software LibrariesRSA - EC – SHA-2 – Toolbox,Infineon Technologies AG, Chipcard and Security, Evaluation Documentation, certifiedunderGermanSchemewithcertificationreport - BSI-DSZ-CC-0640