TÜBİTAK BİLGEM UEKAE

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

eID Technologies Unit

# SECURITY TARGET LITE

of

AKIS GEZGIN_I v1.1.0.0

BAC Configuration with Active Authentication

| | |
|---|---|
| **Revision no** | 02 |
| **Revision date** | 26.03.2019 |
| **Document code** | AKiS-GEZGiN_I-BAC&AA-ST_Lite-02 |
| **Prepared by** | eID Technologies Unit |
| **Approved by** | AKİS Project Manager |

## REVISION HISTORY

| Revision # | Revision Reason | Date |
|---|---|---|
| 1. | First public version of the ST created | 19.02.2018 |
| 2. | Addition of new card activation method and support for ECC-521 bit curves | 26.03.2019 |

## CONTENTS

Revision History ..... 2

Contents ..... 3

List of Figures ..... 6

List of Tables ..... 7

1 ST Introduction ..... 8

**1.1 ST Reference ..... 8**

**1.2 TOE Reference ..... 8**

**1.3 TOE Overview ..... 8**

1.3.1 TOE type and Usages of the TOE ..... 8

1.3.2 Major Security Properties of the TOE ..... 9

**1.4 Required non-TOE HW/SW/Firmware Available to the TOE ..... 9**

**1.5 TOE Description ..... 10**

1.5.1 Physical and Logical Scope of the TOE ..... 10

1.5.2 Security Features of the TOE ..... 12

1.5.3 Interfaces ..... 14

1.5.4 Life Cycle ..... 14

1.5.5 TOE Configurations ..... 17

1.5.6 Platform Information ..... 17

2 CC Conformance Claim ..... 25

**2.1 PP Claim ..... 25**

**2.2 Package Claim ..... 25**

3 Security Problem Definition ..... 26

**3.1 Assets ..... 26**

3.1.1 Assets Protected by the eMRTD Application ..... 26

**3.2 Subjects and External Entities ..... 27**

**3.3 Threats ..... 29**

3.3.1 Hardware Related Threats ..... 29

3.3.2 Terminal, Communication and Application Related Threats ..... 32

**3.4 Organisational Security Policies ..... 34**

**3.5 Assumptions ..... 35**
4 Security Objectives ..... 37
**4.1 Security Objectives for the TOE ..... 37**
**4.2 Security Objectives for Operational Environment ..... 39**
4.2.1 Issuing State or Organization ..... 39
4.2.2 Receiving State or Organization ..... 41
**4.3 Security Objectives Rationale ..... 42**
5 Extended Components ..... 48
**5.1 Definition of the Family FAU_SAS (Audit Data Storage) ..... 48**
5.1.1 FAU_SAS.1 Audit Storage ..... 48
**5.2 Definition of the Family FCS_RND (Generation of Random Numbers) ..... 49**
5.2.1 FCS_RND.1 Random Number Generation ..... 49
**5.3 Definition of the Family FIA_API (Authentication Proof of Identity) ..... 49**
5.3.1 FIA_API.1 Authentication Proof of Identity ..... 50
**5.4 Definition of the Family FMT_LIM (Limited Capabilities and Availability) ..... 50**
5.4.1 FMT_LIM.1 Limited Capabilities ..... 51
5.4.2 FMT_LIM.2 Limited Availability ..... 51
**5.5 Definition of the Family FPT_EMSEC ..... 52**
5.5.1 FPT_EMSEC.1 TOE Emanation ..... 52
6 Security Requirements ..... 54
**6.1 Overview ..... 54**
**6.2 Security Functional Requirements ..... 55**
6.2.1 Class FAU: Security Audit ..... 56
6.2.2 Class FCS: Cryptographic Support ..... 56
6.2.3 Class FIA: Identification and Authentication ..... 59
6.2.4 Class FDP: User Data Protection ..... 62
6.2.5 Class FMT: Security Management ..... 64
6.2.6 Class FPT: Protection of the TSF ..... 67
**6.3 Security Functional Requirements for Active Authentication Only ..... 68**
**6.4 Security Assurance Requirements ..... 69**
**6.5 Security Requirements Dependencies ..... 70**

6.5.1 Security Functional Requirements Dependencies ..... 70
6.5.2 Security Assurance Requirements Dependencies ..... 73
**6.6 Security Functional Requirements Rationale ..... 73**
**6.7 Security Assurance Requirements Rationale ..... 78**
7 TOE Summary Specification ..... 79
**7.1 SF_PP: Physical Protection ..... 79**
**7.2 SF_DPM: Device Phase Management ..... 79**
**7.3 SF_AC: Access Control ..... 79**
**7.4 SF_SM: Secure Messaging ..... 80**
**7.5 SF_IA: Identification and Authentication ..... 81**
**7.6 Security Functions Rationale ..... 82**
8 Abbreviations and Definitions ..... 84
9 References ..... 86

# LIST OF FIGURES

Figure 1: Generic file system of the TOE ..... 11

Figure 2: Platform hardware ..... 20

# LIST OF TABLES

Table 1: Features supported by the TOE ..... 9
Table 2: Subjects and External Entities of the TOE ..... 27
Table 3: Hardware related threats ..... 29
Table 4: Application related threats ..... 32
Table 5: Composite TOE Policies ..... 34
Table 6: Composite TOE Assumptions ..... 35
Table 7: Security Objectives Rationale ..... 42
Table 8: Coverage of Assumptions, Threats or OSPs with Security Objectives and the Rationales ..... 43
Table 9: List of SFR's ..... 54
Table 10: Dependency of Composite TOE SFRs ..... 70
Table 11: Coverage of TOE Objectives by SFRs ..... 73
Table 12: Coverage of SFRs by TOE Security Features ..... 82

# 1 ST INTRODUCTION

## 1.1 ST REFERENCE

**Title**: Security Target Lite of AKIS GEZGIN_I v1.1.0.0 BAC Configuration with Active Authentication

**Document Version:** 02

**CC Version:** 3.1 (Revision 4)

**Assurance Level:** EAL4 + (ALC_DVS.2)

## 1.2 TOE REFERENCE

The current Security Target refers to the product AKIS GEZGIN_I BAC Configuration with Active Authentication. Version number of the TOE is 1.1.0.0.

## 1.3 TOE OVERVIEW

The Target of Evaluation (TOE) addressed by this security target is AKIS GEZGIN_I BAC Configuration with Active Authentication. This TOE is the composition of the contactless smartcard chips SLE78CLFX3000P and SLE78CLFX4000P of Infineon M7892 B11 platform with embedded software including electronic Machine Readable Travel Document (eMRTD) Application. The aim of this security target is to define the security assurance and functional requirements of the TOE.

In this document, the term “AKIS GEZGIN” refers to “AKIS GEZGIN_I BAC Configuration with Active Authentication”.

The TOE comprises the following:

- the circuitry of the eMRTD’s chip (the integrated circuit, IC)
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software including operating system and eMRTD application,
- the associated guidance documentation.

### 1.3.1 TOE TYPE AND USAGES OF THE TOE

The TOE type is a contactless smart card chip with embedded software including the eMRTD application.

In addition to Basic Access Control (BAC) and Active Authentication (AA), the embedded software also implements Basic Access Protection (BAP), Supplemental Access Control (SAC), Extended Access Control (EAC) and Extended Access Protection (EAP) which are out of the scope of this ST.

**Table 1: Features supported by the TOE**

| Features of the TOE | Support by the TOE | Scope of the ST |
|---|---|---|
| Basic Access Control (BAC) | ✓ | ✓ |
| Active Authentication (AA) | ✓ | ✓ |
| Basic Access Protection (BAP) | ✓ | X |
| Supplemental Access Control (SAC) | ✓ | X |
| Extended Access Control (EAC) | ✓ | X |
| Extended Access Protection (EAP) | ✓ | X |

### 1.3.2 MAJOR SECURITY PROPERTIES OF THE TOE

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks,
- Passive Authentication (PA),
- Active Authentication (AA),
- Basic Access Control (BAC),
- SHA-1, SHA-2/224, SHA-2/256, SHA-2/384, SHA-2/512 Operations,
- True Random Number Generation,
- DES3 Encryption and Decryption,
- Retail MAC (DES3),
- Signature generation with ISO 9796-2 Scheme 1,
- Signature generation with ECDSA.

## 1.4 REQUIRED NON-TOE HW/SW/FIRMWARE AVAILABLE TO THE TOE

None.

## 1.5 TOE DESCRIPTION

### 1.5.1 PHYSICAL AND LOGICAL SCOPE OF THE TOE

A physical TOE will be in form of a paper book or plastic card with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to) personal data of the MRTD holder:

- The biographical data on the biographical data page of the passport book/card,
- The printed data in the Machine-Readable Zone (MRZ) that identifies the MRTD and
- The printed portrait.

The antenna and the plastic or paper, optically readable cover of the travel document, where the chip part of the TOE is embedded in, is not part of the TOE. The tying-up of the chip to the paper or the plastic card is achieved by physical and organizational security measures being out of scope of this ST.

The physical scope of the TOE is composed of the IC dedicated software, the IC embedded software and the IC platform that the embedded software runs on. Please see Section 1.5.6 for more information on the IC platform.

A logical TOE will have data of the TOE holder stored according to the Logical Data Structure as specified by ICAO 9303 [ 11 ] on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the TOE holder.

- The digital MRZ Data,
- The digitized portraits,
- The optional biometric reference data of finger(s) or iris image(s) or both,
- The other data according to Logical Data Structure and
- The Document security object.

In addition, the security functions implemented by the TOE are given in detail in Section 1.3.2.

#### 1.5.1.1 LDS APPLICATION

The Logical Data Structure (LDS) application is a generic file system that can be configured to meet the ICAO 9303 e-Passport Specifications.

The generic file system is given in Figure 1.

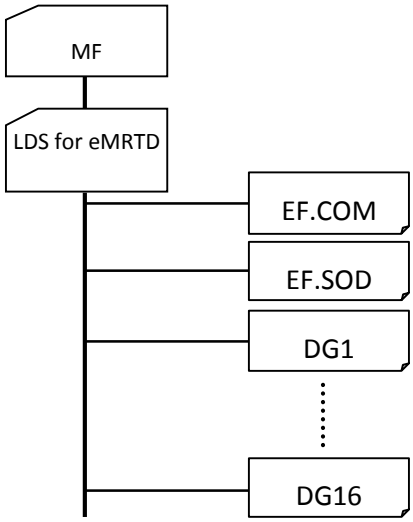



**Figure 1: Generic file system of the TOE**

There are two types of files generated in the LDS application:

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

The application handles the creation and management of the files. These files are located in the EEPROM area of the TOE. Access rights information, file size, file ID (FID) and short file identifier (SFI) are stored in the file header in the EEPROM area.

#### 1.5.1.1.1 SYSTEM FILES

System files are dedicated to store sensitive data that are used by the application. The integrity of the System Files is protected by means of a checksum. These files may be created and updated during the Personalization operation. The keys stored in the files are not readable.

These files are used by the application and shall be created before any use of the application.

In particular, these files are used to store as TSF data:

- Active Authentication private key,
- The keys needed to perform BAC.

#### 1.5.1.1.2 DATA FILES

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

Common Data Files are as follows:

- EF.COM which describes which DGs are present in the file structure,

- EF.SOD which contains the hash values of all data groups (files), a signature over all these hash values along with the corresponding country certificate. It ensures the integrity & authenticity of DGs,
- DG1 up to DG16 which contains information about the holder (picture, name…) and key required to perform authentications.

### 1.5.2 SECURITY FEATURES OF THE TOE

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support as detailed in Section 8,
- Passive Authentication (PA),
- Active Authentication (AA),
- Basic Access Control (BAC),
- The following cryptographic operations for AA:
  - SHA-1, SHA-2/224, SHA-2/256, SHA-2/384, SHA-2/512 Operations,
  - Signature generation with ECDSA,
  - Signature generation with ISO 9796-2 Scheme 1,
  - True Random Number Generation,
- The following cryptographic services for BAC:
  - SHA-1,
  - DES3 Encryption and Decryption,
  - Retail MAC (DES3),
  - True Random Number Generation.

Note that for Active Authentication, the hash operation SHA-2/224 is only used for the signature generation with ECDSA. Note also that the cryptographic operations SHA-1, SHA-2/224, SHA-2/256, SHA-2/384, SHA-2/512, DES3 encryption/decryption, and Retail MAC (DES3) are not accessible to the external world since they are intended for internal use only by the embedded OS and there exists no interface exposing these operations to the external world.

The platform is certified for EAL 6+. The physical protection is mainly inherited from the platform which provides protection against modification, snooping, probing, environmental stress, logical attacks and emanation attacks. The platform is resistant against single shot power analyses attacks, applied with high attack potential. Against more sophisticated attacks, e.g., differential analysis and advanced statistics, appropriate countermeasures are recommended. For detailed information, please see Security IC ST [ 5 ].

The TOE makes use of the crypto library of the platform for RSA and ECC operations which is also certified. It provides protection against SPA, DPA and DFA attacks.

#### 1.5.2.1 PASSIVE AUTHENTICATION (PA)

Passive Authentication (PA) ensures that the contents of the TOE is authentic and tamper-proof and has not changed since personalization. The TOE contains a file (SOD), placed under the corresponding application during personalization. This SOD file, located under the eMRTD application, stores the hash values of all data groups (files), a signature over all these hash values along with the corresponding country certificate. PA is enforced by the TOE environment, i.e., if the TOE environment checks the authenticity of the TOE by PA, it calculates the hash value of all files stored under the corresponding application. Modification of the files would be detected by the TOE environment by comparing the stored hash value against the calculated hash value.

#### 1.5.2.2 ACTIVE AUTHENTICATION (AA)

Active Authentication (AA) prevents cloning of e-passport chips. For this purpose, TOE contains an RSA or ECC private key in its secure memory that cannot be read or copied, nevertheless its existence could be proven. The personalization agent decides what key to use for AA based on governmental policies. By using a challenge-response mechanism, TOE signs the data provided by the TOE environment therefore proving that TOE contains the private component of the RSA or ECC key whose public component is already stored in data group 15 (DG15).

Active authentication prevents TOE cloning. Since the PA guarantees that the contents of the TOE is authentic and has not changed, the combination of PA and AA proves the authenticity and unclonability of the TOE.

#### 1.5.2.3 BASIC ACCESS CONTROL (BAC)

Basic Access Control (BAC) is a mechanism used in e-passports that prevents chip skimming and eavesdropping on the communication between the TOE and the TOE environment by encrypting the transmitted information. Before any data can be read from the TOE, the TOE environment needs to prove that it has physical access to the TOE by using a session key derived from the Machine Readable Zone (MRZ) of the TOE.

BAC ensures that only authorized parties can wirelessly read personal information from e-passports with an RFID chip. Thus the attackers cannot eavesdrop on the information transmitted between the TOE and the TOE environment.

### 1.5.3 INTERFACES

**For the electrical I/O:**

- ISO 1177 - Information Processing Character Structure For Start/Stop And Synchronous Character Oriented Transmission [ 30 ],
- ISO 14443-3 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 3: Initialization and anticollision [ 31 ],
- ISO 14443-4 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 4: Transmission protocol [ 32 ].

**For the commands:**

- ISO 7816 Commands [ 33 ], [ 34 ], [ 35 ],
- MRTD Commands [ 15 ].

### 1.5.4 LIFE CYCLE

This Security Target is conformant to the protection profile BSI-CC-PP-0055 and life cycles of the composite product AKIS GEZGIN are based on the life cycles of platform ST and given as follows. Note that any TOE-specific details are given in *italics*.

**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, the eMRTD 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 chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories. 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.
- If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM)[1].
- **(Step4)** The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book/*card*.
- **(Step5)** The MRTD manufacturer (i) creates the MRTD application (create MF and LDS) and (ii) equips the chips with pre-personalization Data.
    - ***(Activation)*** *AKIS GEZGIN is activated in this phase. Initialization key and personalization key are loaded in this step. TOE accepts only PERFORM SECURITY OPERATION (PSO) command, activation command and some commands that provide very limited information about TOE in this phase. Before the activation command, activation agent is to transfer activation public key, in the same session, to the TOE via PSO: VERIFY CERTIFICATE command. Managed by activation agent, this phase is ended by activation operation in which a 2048-bit cryptogram created using activation private key is sent to the TOE via EXCHANGE CHALLENGE command. If the cryptogram is verified successfully, activation is completed and the composite TOE (card) becomes ready for initialization.*[2]
    - ***(Initialization)*** *After successful authentication of initialization key, another successful authentication is needed to complete this step. File structure is created during this step.*
- 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.

1 For the composite product AKIS GEZGIN, the IC embedded software hex code is always preloaded onto the flash memory of the chip platform during mass production by the IC manufacturer.
2 Before activation, the IC embedded software can be removed from IC, for further version upgrades, by the MRTD manufacturer using a cryptogram intended for flash loader activation only.

**Phase-3: Personalization of the MRTD**

- **(Step6)** *This phase starts with the successful authentication of personalization key. Another successful authentication is needed to complete this phase. Personal information data are written and access rules are defined in this phase. Application specific restrictions cannot be implemented in personalization phase.*
- 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 if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (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.

**Phase-4: Operational Use**

- **(Step7)** The TOE is used as MRTD's chip by the user 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.

***Phase-5: Death Phase***

- *Death phase is defined by embedded software. The TOE becomes out of order and can't be used as a legitimate one. The TOE enters this phase if unsuccessful authentication attempts occur during activation, initialization and personalization operations. In addition, upon detection of critical integrity errors in operational use, the TOE enters the death phase. In this phase, the TOE doesn't accept any commands but the ones that provide limited information about itself.*

### 1.5.5 TOE CONFIGURATIONS

AKIS GEZGIN_I BAC configuration with Active Authentication is within the scope of this Security Target. The configuration is done through writing to a special area in the EEPROM area during the Personalization Operation.

### 1.5.6 PLATFORM INFORMATION

#### 1.5.6.1 PLATFORM IDENTIFICATION

**Platform:**

- Infineon Technologies, SLE78CLFX3000P and SLE78CLFX4000P

**Platform ST:**

- Security Target Lite M7892 B11 Recertification Including Optional Software Libraries RSA – EC – SHA2 – Toolbox; Common Criteria CCv3.1 EAL6 Augmented (EAL6+) Resistance to Attackers with High Attack Potential; Version 0.3, 2015-10-13 [0782v2b_pdf.pdf can be found on commoncriteriaportal.org]

**Platform PP Conformance:**

- Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

**Platform Assurance Level:**

- EAL6 + ALC_FLR.1

**Platform Certification Report:**

- BSI-DSZ-CC-0782-V2-2015, 03.11.2015 [0782V2a_pdf.pdf can be found on commoncriteriaportal.org]

**Common Criteria Version:**

- CC v3.1 Revision 4

**Platform Features:**

- 24-bit linear addressing,
- up to 16 MByte of addressable memory,
- register based architecture,
- 2-stage instruction pipeline,

- extensive set of powerful instructions, including 16 and 32-bit arithmetic and logic instructions,
- CACHE with single-cycle access searching,
- 16-bit ALU.

**Configuration of AKIS GEZGIN Platform:**

- contactless communication ISO 14443-3 type A,
- flash loader unlocked: ES is loaded to the IC by Infineon but flash loader functionality is still delivered with the IC to be locked by card issuer,
- RAM: 8K,
- total flash memory: 300KB for SLE78CLFX3000P, 404KB for SLE78CLFX4000P,
- FLASH memory dedicated for ES: 192 KB,
- FLASH memory dedicated for user data: 88KB for SLE78CLFX3000P, 184KB for SLE78CLFX4000P,
- with RSA 2048, RSA 4096 and SHA-2 libraries,
- with EC and toolbox libraries.

**Configuration of M7892:**

- software libraries RSA 2048 v1.02.013, RSA 4096 v1.02.013, SHA-2 v1.01,
- guidance documentation;
  - M7982 Controller Family for Security Applications,
  - SLX 70 Family Production and Personalization, User's Manual,
  - SLE 70 Family Programmer's Reference User's Manual,
  - SLE 70 Asymmetric Crypto Library Crypto@2304T, RSA / ECC / Toolbox, User's Interface,
  - Chip card and Security ICs, SLx70 Family Secure Hash Algorithm SHA-2,
  - Crypto@2304 T User Manual,
  - M7892 Controller Security Guidelines User Manual,
  - M7892 Controller Family for Security Applications, Errata Sheet.

#### 1.5.6.2 PLATFORM HARDWARE

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture.

The block diagram of the platform is given in Figure. The major components are stated below.

**Core:**

- two CPUs,
- MMU (Memory Management Unit),
- MED (Memory Encryption Decryption),
- EDU (Error Detection Unit),
- CACHE with post failure detection.

**Memory:**

- ROM (not user accessible),
- Infineon SOLID FLASH Memory [EEPROM],
- RAM.

**Cryptographic Co-Processors:**

- SCP (Symmetric co-processor) [AES, TDES – two keys and three keys],
- Crypto2304T [RSA-2048 bit, RSA-4096 bit with CRT, EC].

**Bus systems:**

- a memory bus,
- a peripheral bus for high speed communication with peripherals.

**Peripherals:**

- true random NUMBER GENERATOR (TRNG),
- deterministic random number generator (DRNG),
- timers,
- watchdog,
- universal asynchronous receiver/transmitter (UART),
- checksum module (CRC).

**Control:**

- dynamic power management,
- internal clock oscillator,
- interrupt and peripheral event channel controller (ITP and PEC),
- interface management module (IMM).

**Security Modules:**

- operation within the specified range (frequency sensor),

- alarms,
- user mode security life control (UmSLC),
- voltage regulator.

**Infineon® SOLID FLASH:**

The flexible memory concept consists of ROM and flash memory as part of the non-volatile memory (NVM), respectively Infineon SOLID FLASH. For the Infineon SOLID FLASH memory the unified channel programming (UCP) memory technology is used.

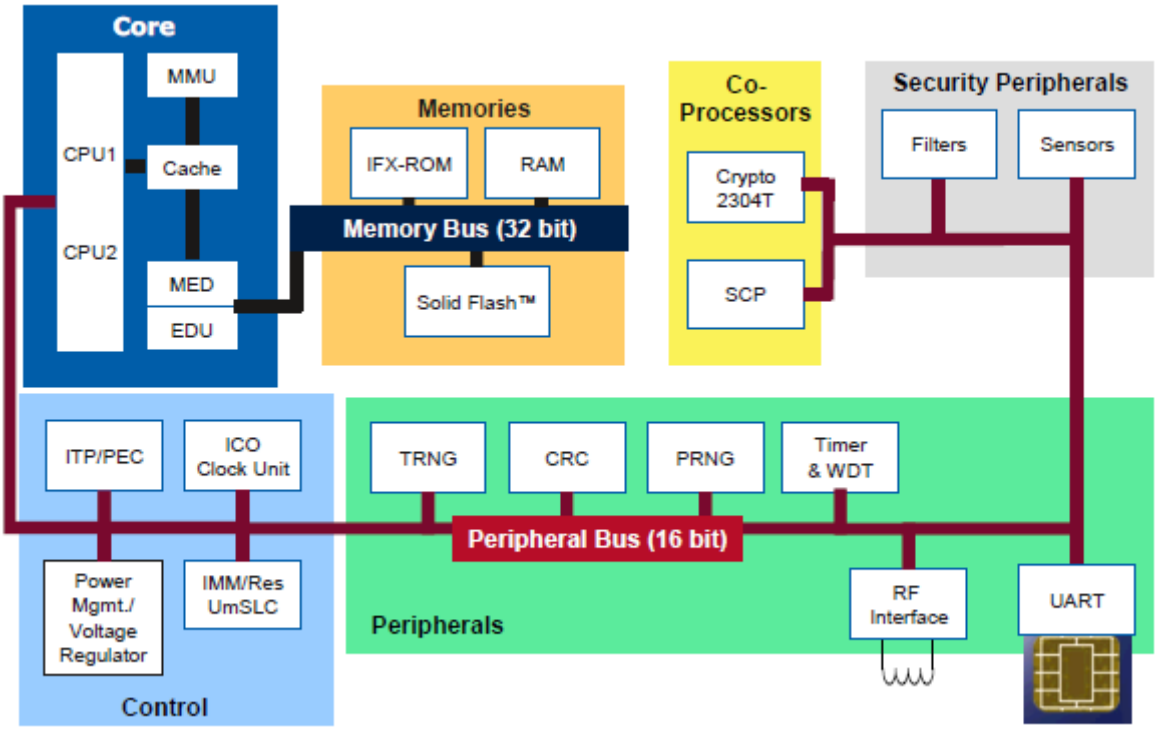



**Figure 2: Platform hardware**

### 1.5.6.3 PLATFORM FIRMWARE

The firmware parts are RMS Library, the SAM, the STS and the flash loader.

**RMS Library:**

The RMS library provides some functionality via an API to the Smartcard Embedded Software such as Infineon® SOLID FLASH™ service routines.

**STS (Self Test Software):**

The STS is implemented in a separated TEST-ROM being part of the platform. The STS firmware is used for test purposes during start-up.

**SAM (Service Algorithm Module):**

SAM provides functionality for the tearing save write into the Infineon SOLID FLASH.

**Flash Loader:**

Flash loader allows downloading the embedded operating system to the Infineon SOLID FLASH during the manufacturing process. Infineon AG provides following possibilities for the card issuer to download their software to the IC:

- Infineon downloads the user software during the IC production phase.
- Infineon may supply the IC without the ES, in this case ES is not delivered to Infineon.
- Infineon downloads the parts of the ES and Card Issuer completes the rest

#### 1.5.6.4 PLATFORM SOFTWARE

Platform software consists of RSA, SHA-2 and base libraries and they are delivered as object code. They are also delivered securely to the AKİS Project Group.

**RSA Library:**

The RSA library is used to provide a high level interface to RSA cryptography implemented on the hardware component Crypto2304T.
RSA library has protection against SPA, DPA, DFA attacks.

**EC Library:**

The EC library is used to provide a high level interface to EC cryptography implemented on the hardware component Crypto2304T.
EC library has protection against SPA, DPA, DFA attacks.

**SHA-2 Library:**

The SHA-2 library provides the calculation of a hash value of given input. SHA-2 is intended to be used for signature generation, verification and generic data integrity checks.

**BASE Library:**

The base library provides the low level interface to the asymmetric cryptographic coprocessor and has no user available interface. The base library does not provide any security functionality, implements no security mechanism, and does not provide additional specific security functionality.

#### 1.5.6.5 PLATFORM INTERFACES

**External Interfaces:**

- The physical interface of the TOE to the external environment, that is the entire surface of the IC,
- The electrical interface of the TOE to the external environment that is constituted by the pads of the chip, RES, I/O, CLK lines and supply lines VCC and GND,
- The data-oriented I/O interface to the TOE that is formed by the I/O pad,
- ISO 7816-3 Cards with contacts, electrical interface and transmission protocols.

**ES Interfaces:**

- Special function registers [Interface to the firmware] which are used for general configuration purposes and chip configuration,
- The interface of the platform to the ES which is constituted on one hand by the RMS routine calls and on the other by the instruction set of the platform,
- The interface of the platform to test routines, formed by STS test routine call,
- The interface to the RSA and SHA-2 that are defined from RSA and SHA-2 library interfaces.

#### 1.5.6.6 PLATFORM SECURITY SERVICES

##### 1.5.6.6.1 RANDOM NUMBER GENERATOR

**Physical random number generator:**

Quality metric is AIS31 PTG.2 (Functionality Classes and Evaluation Methodology for Physical Random Number Generators – Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik respectively “A proposal for: Functionality classes for random number generators”, Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik).

**Deterministic random number generator:**

Out of the scope for certification.

##### 1.5.6.6.2 RSA FUNCTIONALITY

**RSA library:**

The RSA library is used to provide a high level interface to RSA cryptography implemented on the hardware component Crypto2304T.

RSA library has protection against SPA, DPA, DFA attacks.

**RSA Routines:**

- CryptoRsaVerify (RSA signature verification),
- CryptoRsaSignCrt (RSA signature generation).

#### 1.5.6.6.3 EC FUNCTIONALITY

**EC library:**

The EC library is used to provide a high level interface to EC cryptography implemented on the hardware component Crypto2304T.
EC library has protection against SPA, DPA, DFA attacks.

**EC Routines:**

- ECC_Add (primitive ECC operations like ECC Add and ECC Double),
- ECC_DH (Diffie-Hellman key exchange protocol),
- ECC_ECDSASign (ECDSA signature generation),
- ECC_ECDSAVer (ECDSA signature verification).

#### 1.5.6.6.4 DES FUNCTIONALITY

The TOE supports the encryption and decryption in accordance with the specified algorithm TDES with cryptographic key sizes of 112 bits or 168 bits.

#### 1.5.6.6.5 SHA LIBRARY

The SHA-library provides the calculation of a hash value of given input. SHA-2 is intended to be used for signature generation, verification and generic data integrity checks.

### 1.5.6.7 PLATFORM SECURITY FEATURES

**Integrity Guard Concept:**

This new product family features a progressive security philosophy focusing on the data integrity. This new concept is based on three main principles:

- full error detection,
- full encryption,
- intelligent active shielding.

#### 1.5.6.7.1 FULL ON-CHIP ENCRYPTION

The TOE provides full on-chip encryption covering the complete core, busses, memories and cryptographic co-processors leaving no plaintext on the chip.

Encrypted signals have no use for an attacker neither for manipulation nor probing (probing and emission monitoring).

#### 1.5.6.7.2 ERROR DETECTION

**Operation errors:**

- double CPU.

**Memory errors:**

- SOLID FLASH EDC and ECC (one bit and two bits respectively),
- RAM EDC,
- Cache.

#### 1.5.6.7.3 INTELLIGENT ACTIVE SHIELDING

An intelligent shielding finishes the upper layers above security critical signals and wires, finally providing the so called "$I^2$ Shield".

# 2 CC CONFORMANCE CLAIM

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

As conformance claim is as follows:

- part 2 extended,
- part 3 conformant.

## 2.1 PP CLAIM

This ST claims strict conformance to BSI-CC-PP-0055, version 1.10, 25th March 2009.

## 2.2 PACKAGE CLAIM

The current ST is conformant to the following security requirements package: assurance package EAL4 augmented with ALC_DVS.2 as defined in the CC, part 3.

# 3 SECURITY PROBLEM DEFINITION

The security problem definition is based on the protection profile BSI-CC-PP-0055 to which this ST is strictly conformant. Since the TOE also supports the Active Authentication, a corresponding threat for counterfeitness has been added. The TOE is the composition of the Embedded Software (ES) and the security IC. ES also includes the eMRTD Application.

The assets, subjects & external entities, threats, organizational security policies and the assumptions are given in the following sections.

## 3.1 ASSETS

### 3.1.1 ASSETS PROTECTED BY THE EMRTD APPLICATION

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

#### 3.1.1.1 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 [ 11 ]. 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.DG16 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.

Due to interoperability reasons as the 'ICAO Doc 9303' [ 11 ] the TOE described in this security target specifies only 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),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

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.

#### 3.1.1.2 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.

## 3.2 SUBJECTS AND EXTERNAL ENTITIES

This ST considers the subjects given in Table 2.

**Table 2: Subjects and External Entities of the TOE**

| Subject | Definition |
|---|---|
| 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 defined in [ 11 ]. |
| Terminal | A terminal is any technical system communicating with the TOE through the contactless interface. |

| Subject | Definition |
|---|---|
| Inspection system (IS) | A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the user and verifying its authenticity and (ii) verifying the traveler as MRTD holder.<br>The Basic Inspection System (BIS) :<br>• contains a terminal for the contactless communication with the MRTD's chip,<br>• implements the terminals part of the BAC and/or AA Mechanisms,<br>• 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/card providing this information.<br>The General Inspection System (GIS)[3]:<br>GIS is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.<br>The Extended Inspection System (EIS):<br>In addition to the General Inspection System,<br>• implements the Terminal Authentication Protocol and<br>• is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.<br>The security attributes of the EIS are defined of the Inspection System Certificates. |
| 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[4] | 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), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD. |

3 This security target does not distinguish between the BIS, GIS and EIS because the Extended Access Control is out of scope.

## 3.3 THREATS

### 3.3.1 HARDWARE RELATED THREATS

Threats related to hardware are given in Table 3. These threats are taken from the platform ST [ 5 ].

**Table 3: Hardware related threats**

| # | Threat | Definition |
|---|---|---|
| 1. | 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.<br>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.<br>Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. |

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

| | | |
|---|---|---|
| | | Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF. |
| 2. | T.Information_Leakage: Information Leakage from the 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.<br>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).<br>Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.<br>Asset: confidentiality of logical MRTD and TSF data |
| 3. | 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.<br>This may be achieved, e.g., by operating the 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.<br>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 |
| 4. | 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.<br>This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.<br>Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD.<br>Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF. |
| 5. | T.Counterfeit: Production of unauthorized copies or reproductions of genuine MRTD’s chips | Adverse action: An attacker produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as the chip of a counterfeit MRTD. The attacker may either (i) generate a new data set from scratch or (ii) extract completely or partially the data from a genuine MRTD's chip and then copy them on another chip to imitate the genuine MRTD's chip.<br>Threat agent: having high attack potential, being in possession of one or more legitimate MRTDs and blank MRTDs.<br>Asset: authenticity of the MRTD’s chip |

### 3.3.2 TERMINAL, COMMUNICATION AND APPLICATION RELATED THREATS

Terminal, communication and application related threats are given in Table 4.

**Table 4: Application related threats**

| # | Threat | Definition |
|---|---|---|
| 1. | 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.<br>Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.<br>Asset: Anonymity of user. |
| 2. | 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.<br>Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance.<br>Asset: confidentiality of logical MRTD data. |
| 3. | 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.<br>Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance<br>Asset: confidentiality of logical MRTD data |

| | | |
|---|---|---|
| 4. | 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.<br>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/card, 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.<br>Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs.<br>Asset: authenticity of logical MRTD data |

## 3.4 ORGANISATIONAL SECURITY POLICIES

Organizational security policies of the composite TOE is given in Table 5.

**Table 5: Composite TOE Policies**

| # | Policy Name | Definition |
|---|---|---|
| 1. | 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. |
| 2. | 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. |
| 3. | P.Personal_Data: Personal data protection policy | The biographical data and their summary printed in the MRZ and stored on MRTD's chip, the printed portrait and the digitized portrait, the biometric reference data of finger(s), the biometric reference data of iris image(s) and data according to LDS stored on the MRTD's chip are personal data of the MRTD holder.<br>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 chip shall provide the possibility for the BAC to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ 11 ]. (Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.) |

## 3.5 ASSUMPTIONS

Assumptions for the operational environment of the composite TOE is given in Table 6. All except A.Pers_Agent_AA and A.Insp_Sys_AA are taken from the PP [ 2 ].

**Table 6: Composite TOE Assumptions**

| # | Assumption Name | Definition |
|---|---|---|
| 1. | 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 the manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). |
| 2. | A.MRTD_Delivery: Delivery of the MRTD during steps 4 to 6 | Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:<br>- Procedures shall ensure protection of TOE material/information under delivery and storage.<br>- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.<br>- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill. |
| 3. | 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.<br>The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms. |

| # | Assumption Name | Definition |
|---|---|---|
| 4. | A.Insp_Sys: Inspection Systems for global interoperability | The Inspection System is used by the border control officer of the receiving State for eMRTD (i) examining an MRTD presented by the user 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 [ 11 ] The Basic Inspection System reads the logical MRTD under BAC and performs the Passive Authentication to verify the logical MRTD. |
| 5. | A.BAC-Keys: Cryptographic quality of BAC Keys | The Document BAC 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" [ 11 ], the Document BAC 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. |
| 6. | A.Pers_Agent_AA: Personalization of the MRTD's chip including Active Authentication | The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip.<br>The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by mechanisms mentioned in A.Pers_Agent. |
| 7. | A.Insp_Sys_AA: Inspection Systems for global interoperability with Active Authentication | The Inspection System may also implement the terminal part of the Active Authentication Protocol if it wants to ensure the TOE is not cloned. |

# 4 SECURITY OBJECTIVES

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

The security objectives are based on the protection profile BSI-CC-PP-0055 to which this ST is strictly conformant. Since the TOE also supports the Active Authentication, a corresponding security objective for chip authenticity has been added.

## 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[5]**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ 11 ] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

**OT.Data_Int: Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. 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

5 The OT.AC_Pers implies that (1) the data of the LDS groups written during personalization for MRTD holder can not be changed by write access after personalization, (2) the Personalization Agents may (i) add (fill) data into the LDS data groups, and (ii) update and sign the Document Security Object accordingly. Since the TOE also supports EAC, the authorized terminals are allowed to update only EF.CVCA in the "Operational Use" phase in cases where link certificates are successfully verified by the TOE.

authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

**OT.Identification: 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 successfully authenticated Basic Inspection System or Personalization Agent.

The following TOE security objectives address the protection provided by the MRTD’s chip independent 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 IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

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

**OT.Prot_Inf_Leak: 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.

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

**OT.Chip_Authenticity: Protection against forgery**

The TOE must support the Inspection Systems so that they can verify the authenticity of the MRTD's chip. In order to prove its identity, the TOE stores an RSA or EC private key which is used for Chip Authentication. This mechanism is described as "Active Authentication".

## 4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

### 4.2.1 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 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 according to [ 11 ].

**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' [11], 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.

**OE.Active_Auth_Key: Active Authentication Key**

The issuing State or Organization may establish the necessary public key infrastructure in order to:

- Generate the MRTD's Active Authentication Key Pair,
- Sign and store the Active Authentication Public Key in EF.DG15,
- Store the Active Authentication Private Key in secure memory,
- Support inspection systems of receiving States or Organizations to verify the authenticity of the MRTD's chip by certification of the Active Authentication Public Key by means of the Document Security Object.

### 4.2.2 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/card**

The inspection system of the receiving State or Organization must examine the MRTD presented by the user 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 [ 11 ].

**OE.Passive_Auth_Verif: Verification by Passive Authentication**

The border control officer of the receiving State for eMRTD 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 under BAC will use inspection systems which implement the terminal part of the BAC and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e., Basic Inspection Systems).

**OE.Exam_MRTD_AA: Examination of the MRTD passport book/card using Active Authentication**

During examination of the MRTD presented by the traveler, the basic inspection system may follow the Active Authentication Protocol to verify the authenticity of the MRTD's chip.

## 4.3 SECURITY OBJECTIVES RATIONALE

**Table 7: Security Objectives Rationale**

| | 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 | OT.Chip_Authenticity | OE.MRTD_Manufact | OE.MRTD_Delivery | OE.Personalization | OE.Pass_Auth_Sign | OE.BAC-Keys | OE.Active_Auth_Key | OE.Exam_MRTD | OE.Passive_Auth_Verif | OE.Prot_Logical_MRTD | OE.Exam_MRTD_AA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.Phys-Tamper | | | | | | | X | | | | | | | | | | | | |
| T.Information_Leakage | | | | | | X | | | | | | | | | | | | | |
| T.Malfunction | | | | | | | | X | | | | | | | | | | | |
| T.Abuse-Func | | | | | X | | | | | | | X | | | | | | | |
| T.Counterfeit | | | | | X | X | X | X | X | | | | | | X | | | | X |
| T.Chip_ID | | | | X | | | | | | | | | | X | | | | | |
| T.Skimming | | | X | | | | | | | | | | | X | | | | | |
| T.Eavesdropping | | | X | | | | | | | | | | | | | | | | |
| T.Forgery | X | X | | | | | X | | | | | | X | | | X | 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 | | | | | |
| A.Pers_Agent_AA | | | | | | | | | | | | X | | | | | | | |
| A.Insp_Sys_AA | | | | | | | | | | | | | | | | | | | X |

**Table 8: Coverage of Assumptions, Threats or OSPs with Security Objectives and the Rationales**

| Threats / OSPs / Assumptions | Corresponding Objectives | Rationale |
|---|---|---|
| T.Phys-Tamper | OT.Prot_Phys-Tamper | 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.<br><br>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". |
| T.Information_Leakage | OT.Prot_Inf_Leak | |
| T.Malfunction | OT.Prot_Malfunction | |
| T.Abuse-Func | OT.Prot_Abuse-Func, OE.Personalization | The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks using the platform IC as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to holder to disclose or to manipulate the logical MRTD.<br><br>This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality".<br><br>Additionally this objective is supported by the security objective for the TOE environment:<br><br>**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 the holder are enabled according to the intended use of the TOE. |
| T.Chip_ID | OT.Identification, OE.BAC-Keys | The threat **T.Chip_ID** "Identification of the chip" addresses the trace of the MRTD movement by identifying remotely platform IC through the contactless communication interface.<br><br>This threat is countered as described by the security objective **OT.Identification** by BAC using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**. |
| T.Skimming | OT.Data_Conf, OE.BAC-Keys | The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping** "Eavesdropping to the communication between |
| T.Eavesdropping | OT.Data_Conf | |

| Threats / OSPs / Assumptions | Corresponding Objectives | Rationale |
|---|---|---|
| | | TOE and inspection system" address the reading of the logical MRTD trough the contactless interface or listening the communication between the platform IC and a terminal.<br><br>This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through BAC using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**. |
| T.Forgery | OT.AC_Pers,<br>OT.Data_Int,<br>OT.Prot_Phys-Tamper,<br>OE.Pass_Auth_Sign,<br>OE.Exam_MRTD,<br>OE.Passive_Auth_Verif | 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.<br><br>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**).<br><br>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/card according to **OE.Exam_MRTD** "Examination of the MRTD passport book/card" shall ensure that passport book/card does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD.<br><br>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". |
| T.Counterfeit | OT.Prot_Abuse-Func,<br>OT.Prot_Inf_Leak,<br>OT.Prot_Phys-Tamper,<br>OT.Prot_Malfunction,<br>OT.Chip_Authenticity,<br>OE.Exam_MRTD_AA,<br>and<br>OE.Active_Auth_Key | The threat **T.Counterfeit** "Production of unauthorized copies or reproductions of genuine MRTD's chips" addresses the attack of generating unauthorized copies or reproductions of genuine MRTD's chips. This attack is countered by a set of objectives that ensure MRTD's chip data are not copied from the TOE: **OT.Prot_Abuse-Func**, **OT.Prot_Inf_Leak**, **OT.Prot_Phys-Tamper**, and **OT.Prot_Malfunction**. Additionally, when the TOE is configured so that the eMRTD supports Active |

| Threats / OSPs / Assumptions | Corresponding Objectives | Rationale |
|---|---|---|
| | | Authentication, the TOE addresses extra protections against this threat by proving the authenticity of the MRTD's chip as required by **OT.Chip_Authenticity** using an authentication key pair generated by the issuing State or Organisation (see **OE.Active_Auth_Key**). In this case, **OT.Chip_Authenticity** "Protection against forgery", **OE.Exam_MRTD_AA** "Examination of the MRTD passport book/card using Active Authentication" and **OE.Active_Auth_Key** "Active Authentication Key" all participate in the detection of counterfeit MRTD's chip by the inspection system. |
| P.Manufact | OT.Identification | The OSP **P.Manufact** "Manufacturing of the MRTD's chip" requires a unique identification of the platform IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification.** |
| P.Personalization | OT.AC_Pers, OT.Identification, OE.Personalization | 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".<br><br>Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE".<br><br>The security objective **OT.AC_Pers** limits the management of TSF data and management of TSF to the Personalization Agent. |
| P.Personal_Data | OT.Data_Int, OT.Data_Conf | 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 BAC 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 |

| Threats / OSPs / Assumptions | Corresponding Objectives | Rationale |
|---|---|---|
| | | transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality. |
| A.MRTD_Manufact | OE.MRTD_Manufact | 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. |
| A.MRTD_Delivery | OE.MRTD_Delivery | 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. |
| A.Pers_Agent | OE.Personalization | 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. |
| A.Insp_Sys | OE.Exam_MRTD, OE.Prot_Logical_MRTD | The examination of the MRTD passport book/card addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book/card". 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 BAC and to protect the logical MRTD data during the transmission and the internal handling. |
| A.BAC-Keys | OE.BAC-Keys | The assumption A.BAC-Keys "Cryptographic quality of Basic Access Control Keys and Basic Access Protection Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Cryptographic quality of BAC Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization. |
| A.Pers_Agent_AA | OE.Personalization | The assumption **A.Pers_Agent_AA** "Personalization of the MRTD's chip including |

| Threats / OSPs / Assumptions | Corresponding Objectives | Rationale |
|---|---|---|
| | | Active Authentication" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the protection with a digital signature (SOD signing), the storage of the MRTD holder personal data and the support of Active Authentication protocol according to the decision of the issuing State or Organization. |
| A.Insp_Sys_AA | OE.Exam_MRTD_AA | The examination of the MRTD passport book/card addressed by the assumption **A.Insp_Sys_AA** "Inspection Systems for global interoperability with Active Authentication" is covered by the security objective for the TOE environment **OE.Exam_MRTD_AA** "Examination of the MRTD passport book/card using Active Authentication" that requires the Basic Inspection System to implement and to enforce Active Authentication of the MRTD as part of the MRTD's inspection. |

# 5 EXTENDED COMPONENTS

The extended components defined and described for the TOE are:

- Family FAU_SAS (Audit Data Storage),
- Family FCS_RND (Generation of Random Numbers),
- Family FIA_API (Authentication Proof of Identity),
- Family FMT_LIM (Limited capabilities and availability),
- Family FPT_EMSEC TOE Emanation.

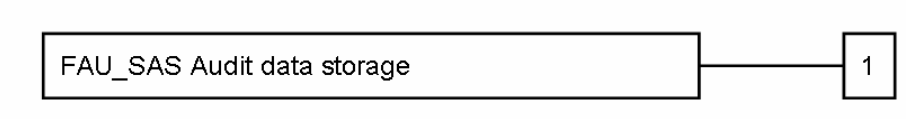
## 5.1 DEFINITION OF THE FAMILY FAU_SAS (AUDIT DATA STORAGE)

FAU_SAS family of the Class FAU (Security Audit) is defined in the platform PP document [ 2 ] and describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

**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.

### 5.1.1 FAU_SAS.1 AUDIT STORAGE

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

Dependencies: No dependencies.

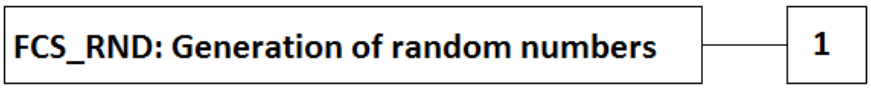
## 5.2 DEFINITION OF THE FAMILY FCS_RND (GENERATION OF RANDOM NUMBERS)

FCS_RND of the Class FCS (cryptographic support) is defined in platform PP document [ 2 ]. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike components FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

**Family behavior**

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

**Component leveling:**




FCS_RND.1 requires that the random number generator implements defined security capabilities and that the 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.

### 5.2.1 FCS_RND.1 RANDOM NUMBER GENERATION

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1: The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

## 5.3 DEFINITION OF THE FAMILY FIA_API (Authentication Proof of Identity)

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

**Application Note 1:** 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. [ 7 ], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

**Family behavior**

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

**Component leveling:**


FIA_API.1 requires the TOE to provide the ability to prove its 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: FIA_API.1**

There are no actions defined to be auditable.

### 5.3.1 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 (Limited Capabilities and Availability)

FMT_LIM of the Class FMT (Security Management) is defined as given in the PP document [ 2 ]. This family describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

**Family behavior**

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

**Component leveling:**


FMT_LIM.1 “Limited capabilities” requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 “Limited availability” requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

**Management: FMT_LIM.1, FMT_LIM.2**

There are no management activities foreseen.

**Audit: FMT_LIM.1, FMT_LIM.2**

There are no actions defined to be auditable.

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

### 5.4.1 FMT_LIM.1 LIMITED CAPABILITIES

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

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

### 5.4.2 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 [assignment: *Limited capability and availability policy*].

## 5.5 DEFINITION OF THE FAMILY FPT_EMSEC

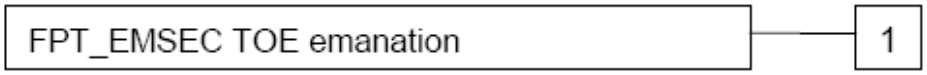
FPT_EMSEC (TOE emanation) of the Class FPT (Protection of the TSF) is defined as given in PP Document [ 2 ].

The TOE shall prevent attacks against TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by other functional requirements defined in Common Criteria Part2.

**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 enabling access to TSF data or user data.

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

**Management: FPT_EMSEC.1**

There are no management activities foreseen.

**Audit: FPT.EMSEC.1**

There are no actions defined to be auditable.

### 5.5.1 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 types of TSF data*] and [assignment list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment*: type of connection*] to gain access to [assignment: *list of type of user data*].

# 6 SECURITY REQUIREMENTS

## 6.1 OVERVIEW

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [ 6 ]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/" and the iteration indicator after the component identifier.

Those parts of the sentences originally marked as assignments on SFRs that are defined in CC part 2 but marked as selections on the corresponding SFRs in the protection profile BSI-CC-PP-0055 are marked as selections in this ST as well.

TOE security functional requirements of the composite product are listed in Table 9 and given in Sections 6.2 and 6.3.

**Table 9: List of SFR's**

| SFR | Explanation |
|---|---|
| FAU_SAS.1 | Audit storage |
| FCS_CKM.1 | Cryptographic Key Generation - Generation of Document Basic Access Keys by the TOE |
| FCS_CKM.4 | Cryptographic Key Destruction - MRTD |
| FCS_COP.1/SHA | Cryptographic Operation - Hash for Key Derivation |
| FCS_COP.1/ENC | Cryptographic Operation - Encryption/Decryption Triple DES |
| FCS_COP.1/AUTH | Cryptographic Operation - Authentication |
| FCS_COP.1/MAC | Cryptographic Operation - Retail MAC |

| | |
|---|---|
| FCS_RND.1 | Quality metric for random numbers |
| FIA_UID.1 | Timing of Identification |
| FIA_UAU.1 | Timing of Authentication |
| FIA_UAU.4 | Single Use Authentication Mechanisms |
| FIA_UAU.5 | Multiple Authentication Mechanisms |
| FIA_UAU.6 | Re-Authenticating |
| FIA_AFL.1 | Authentication Failure Handling |
| FDP_ACC.1 | Subset access control – Basic Access Control |
| FDP_ACF.1 | Basic Security attribute based access control – Basic Access Control |
| FDP_UCT.1 | Basic Data Exchange Confidentiality |
| FDP_UIT.1 | Data Exchange Integrity |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security Roles |
| FMT_LIM.1 | Limited capabilities |
| FMT_LIM.2 | Limited availability |
| FMT_MTD.1/INI_ENA | Management of TSF data – Writing of Initialization Data and Pre-personalization Data |
| FMT_MTD.1/INI_DIS | Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data |
| FMT_MTD.1/KEY_WRITE | Management of TSF data – Key Write |
| FMT_MTD.1/KEY_READ | Management of TSF data – Key Read |
| FPT_EMSEC.1 | TOE Emanation |
| FPT_FLS.1 | Failure with Preservation of Secure State |
| FPT_PHP.3 | Resistance to Physical Attack |
| FPT_TST.1 | TSF Testing |
| FIA_API.1/AA | Authentication Proof of Identity – Active Authentication |
| FCS_COP.1/SIG_MRTD | Cryptographic operation |

## 6.2 SECURITY FUNCTIONAL REQUIREMENTS

This ST is strictly conformant to the protection profile BSI-CC-PP-0055; as a result, all the SFRs in the PP are included in this ST. Since the TOE also supports Active Authentication, the SFRs directly related to Active Authentication are given Section 6.3. In addition, some existing SFRs in Section 6.2, e.g., FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, and FPT_EMSEC.1, are refined for Active Authentication.

### 6.2.1 CLASS FAU: SECURITY AUDIT

**FAU_SAS.1 Audit storage**

FAU_SAS.1.1 The TSF shall provide the *IC Manufacturer*[6] with the capability to store *the IC Identification Data*[7] in the audit records.

### 6.2.2 CLASS FCS: CRYPTOGRAPHIC SUPPORT

**FCS_CKM.1 Cryptographic Key Generation - Generation of Document Basic Access Keys by the TOE**

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*[8] and specified cryptographic key sizes *112 bits*[9] that meet the following *ICAO 9303 [ 11 ] normative appendix 5*, A5.2[10].

**FCS_CKM.4 Cryptographic Key Destruction - MRTD**

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *writing first a random path and next all zeros* [11] that meets the following: none[12].

**Application Note 2:** The TOE shall destroy the Triple DES encryption key and the Retail-MAC message authentication key for secure messaging.

**FCS_COP.1/SHA Cryptographic Operation - Hash for Key Derivation**

FCS_COP.1.1/SHA The TSF shall perform *hashing*[13] in accordance with a specified cryptographic algorithm SHA-1, SHA-2/224, SHA-2/256, SHA-2/384, SHA-2/512[14] and cryptographic key sizes *none*[15] that meet the following: U.S. Department of

6 [assignment: authorized users]
7 [assignment: list of audit information]
8 [assignment: cryptographic key generation algorithm]
9 [assignment: cryptographic key sizes]
10 [assignment: list of standards]
11 [assignment: cryptographic key destruction method]
12 [assignment: list of standards]
13 [assignment: list of cryptographic operations]
14 [assignment: cryptographic algorithm]
15 [assignment: cryptographic key sizes]

Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2012-March, section 6.2 SHA-256[16].

**Application Note 3:** The hashing algorithm is defined by the personalization agent during the personalization.

**FCS_COP.1/ENC Cryptographic Operation - Encryption/Decryption Triple DES**

FCS_COP.1.1/ENC The TSF shall perform *secure messaging (BAC) - encryption and decryption*[17] in accordance with a specified cryptographic algorithm *Triple DES in CBC Mode*[18] and cryptographic key sizes *112 bits*[19] that meet the following: *FIPS 46-3 [ 27 ] and ICAO 9303 [ 11 ]; normative appendix 5 A5.3*[20]**.**

**Application Note 4:** 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**

FCS_COP.1.1/AUTH The TSF shall perform *symmetric authentication - encryption and decryption*[21] in accordance with a specified cryptographic algorithm AES[22] and cryptographic key sizes 256 bit[23] that meet the following: FIPS 197 [ 29 ][24]**.**

**Application Note 5:** 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**

FCS_COP.1.1/MAC The TSF shall perform *secure messaging – message authentication code*[25] in accordance with a specified cryptographic algorithm *Retail MAC*[26] and

16 [assignment: list of standards]
17 [assignment: list of cryptographic operations]
18 [assignment: cryptographic algorithm]
19 [assignment: cryptographic key sizes]
20 [assignment: list of standards]
21 [assignment: list of cryptographic operations]
22 [assignment: cryptographic algorithm]
23 [assignment: cryptographic key sizes]
24 [assignment: list of standards]
25 [assignment: list of cryptographic operations]
26 [assignment: cryptographic algorithm]

cryptographic key sizes *112 bits*[27] that meet the following: *ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)*[28].

**Application Note 6:** 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_RND.1 Quality metric for random numbers**

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet:

*PTG.2.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*

*PTG.2.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*

*PTG.2.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*

*PTG.2.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*

*PTG.2.5 The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical proper- ties of the raw random numbers within an acceptable period of time.*

*PTG.2.6 Test procedure A, as defined in [ 36 ] does not distinguish the internal random numbers from output sequences of an ideal RNG.*

*PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997*[29].

27 [assignment: cryptographic key sizes]
28 [assignment: list of standards]

### 6.2.3 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

**FIA_UID.1 Timing of Identification**

FIA_UID.1.1 The TSF shall allow

- *to read the Initialization Data in Phase 2 "Manufacturing",*
- *to read the random identifier in Phase 3 "Personalization of the MRTD",*
- *to read the random identifier in Phase 4 "Operational Use"*[30]

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.

**Application Note 7:** 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.

**FIA_UAU.1 Timing of Authentication**

FIA_UAU.1.1 The TSF shall allow

- *to read the Initialization Data in Phase 2 "Manufacturing",*
- *to read the random identifier in Phase 3 "Personalization of the MRTD",*
- *to read the random identifier in Phase 4 "Operational Use"*[31]

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.

---

29 [assignment: a defined quality metric]
30 [assignment: list of TSF-mediated actions]
31 [assignment: list of TSF mediated actions]

**Application Note 8:** The Basic Inspection System and the Personalization Agent authenticate themselves.

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

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

- *Basic Access Control Authentication Mechanism,*
- *Authentication mechanism based on AES*[32]*.*

**Application Note 9:** The BAC Mechanism is a mutual device authentication mechanism defined in [ 11 ]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip 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.

**FIA_UAU.5 Multiple Authentication Mechanisms**

FIA_UAU.5.1 The TSF shall provide

- *Basic Access Control Authentication Mechanism,*
- Symmetric Authentication Mechanism based on AES[33]

to support user authentication.

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

- *the TOE accepts the authentication attempt as Personalization Agent by* the Symmetric Authentication Mechanism with the Personalization Agent Key*,*
- *the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys*[34]*.*

32 [assignment: identified authentication mechanism(s)]
33 [assignment: list of multiple authentication mechanisms]
34 [assignment: rules describing how the multiple authentication mechanisms provide authentication]

**FIA_UAU.6 Re-Authenticating – Re-authenticating of Terminal by the TOE**

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*[35].

**Application Note 10:** The Basic Access Control Mechanism specified in [ 11 ] 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.

**FIA_AFL.1 Authentication Failure Handling**

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within 1 to 10* [36] unsuccessful authentication attempts occur related to *BAC authentication protocol*[37].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[38], the TSF shall *wait for an administrator configurable time between the receiving the terminal challenge $e_{IFD}$ and sending the TSF response $e_{ICC}$ during the BAC authentication attempts*[39].

**Application Note 11:** The terminal challenge $e_{IFD}$ and the TSF response $e_{ICC}$ are described in [ 15 ], Appendix C. The refinement by inclusion of the word “consecutive” allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the “consecutive unsuccessful authentication attempts” are count independent on power-on sessions but reset to zero after successful authentication only.

35 [assignment: list of conditions under which re-authentication is required]
36 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
37 [assignment: list of authentication events]
38 [selection: met, surpassed]
39 [assignment: list of actions]

### 6.2.4 CLASS FDP: USER DATA PROTECTION

**FDP_ACC.1 Subset access control – Basic Access Control**

FDP_ACC.1.1 The TSF shall enforce the *Basic access control SFP*[40] 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*[41].

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

FDP_ACF.1.1 The TSF shall enforce the *Basic access control SFP*[42] to objects based on the following:

*Subjects:*

- *personalization agent,*
- *basic inspection system,*
- *terminal,*

*Objects:*

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

*Security attributes:*

- *authentication status of terminals*[43].

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

- *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.*

40 [assignment: access control SFP]
41 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
42 [assignment: access control SFP]
43 [assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- *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*[44].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[45].

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

- *Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.*
- *Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.*
- *The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4*[46].

**Application Note 12:** The inspection system needs special authentication and authorization for read access to the data in EF.DGs which are protected by EAC/EAP.

**Application Note 13:** FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

**FDP_UCT.1 Basic data exchange confidentiality - MRTD**

FDP_UCT.1.1 The TSF shall enforce the *Basic access control SFP*[47] to be able to transmit and receive[48] user data in a manner protected from unauthorized disclosure.

**FDP_UIT.1 Data exchange integrity - MRTD**

FDP_UIT.1.1 The TSF shall enforce the *Basic access control SFP*[49] to be able to transmit and receive[50] user data in a manner protected from modification, deletion, insertion and replay[51] errors.

44 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
45 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
46 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
47 [assignment: access control SFP(s) and/or information flow control SFP(s)]
48 [selection: transmit, receive]

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[52] has occurred.

### 6.2.5 CLASS FMT: SECURITY MANAGEMENT

**FMT_SMF.1 Specification of Management Functions**

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

- *initialization,*
- *pre-personalization*
- *personalization*[53]*.*

**Application Note 14:** The management function "initialization" in this SFR is due to the MRTD's chip platform, it is not to be confused with "initialization" step of the TOE life cycle.

**FMT_SMR.1 Security Roles**

FMT_SMR.1.1 The TSF shall maintain the roles

- *manufacturer,*
- *personalization agent,*
- *basic inspection system*[54]*.*

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

**FMT_LIM.1 Limited capabilities**

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: *Deploying test features after TOE delivery does not allow*

- *user data to be manipulated and disclosed,*
- *TSF data to be manipulated and disclosed,*

49 [assignment: access control SFP(s) and/or information flow control SFP(s)]
50 [selection: transmit, receive]
51 [selection: modification, deletion, insertion, replay]
52 [selection: modification, deletion, insertion, replay]
53 [assignment: list of management functions to be provided by the TSF]
54 [assignment: the authorised identified roles]

- *software to be reconstructed and*
- *substantial information about construction of TSF to be gathered which may enable other attacks*[55]*.*

**FMT_LIM.2 Limited availability**

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *Deploying test features after TOE delivery does not allow*

- *user data to be manipulated and disclosed,*
- *TSF data to be manipulated and disclosed,*
- *Software to be reconstructed,*
- *Substantial information about construction of TSF to be gathered which may enable other attacks*[56]*.*

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

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write[57] the *Initialization Data and Pre-Personalization Data*[58] to *the Manufacturer*[59].

**Application Note 15:** 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**

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to *disable read access for users to*[60] the *Initialization Data*[61] to *the Personalization Agent*[62].

55 [assignment: Limited capability and availability policy]
56 [assignment: Limited capability and availability policy]
57 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
58 [assignment: list of TSF data]
59 [assignment: the authorised identified roles]
60 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
61 [assignment: list of TSF data]

**Application Note 16:** According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes 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". The external read access is blocked in the Phase 4 "Operational Use" since it is not needed and may be misused in the Phase 4. The MRTD Manufacturer will write the Pre-personalization Data which is the personalization key.

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

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to write[63] the *Document Basic Access keys*[64] **and Active Authentication Private Key** to *the Personalization Agent*[65].

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[66]the *Document Basic Access Keys,* **Active Authentication Private Key** *and Personalization Agent Keys*[67]to *none*[68].

**Application Note 17:** The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

**Application Note 18:** The Active Authentication Public Key is stored in EF.DG15 and hence access to it is subject to Basic access control SFP.

62 [assignment: the authorised identified roles]
63 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
64 [assignment: list of TSF data]
65 [assignment: the authorised identified roles]
66 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
67 [assignment: list of TSF data]
68 [assignment: the authorised identified roles]

### 6.2.6 CLASS FPT: PROTECTION OF THE TSF

**FPT_EMSEC.1 TOE Emanation**

FPT_EMSEC.1.1 The TOE shall not emit *power variations, timing variations during command execution*[69] in excess of *non-useful information*[70] enabling access to *Personalization Agent Key* **and Active Authentication Private Key**[71] and *none*[72].

FPT_EMSEC.1.2 The TSF shall ensure *any unauthorized users*[73] are unable to use the following interface *smart card circuit contacts* [74] to gain access to *Personalization Agent Key* **and Active Authentication Private Key**[75] and *none*[76].

**FPT_FLS.1 Failure with Preservation of Secure State**

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

- *exposure to out-of-range operating conditions where therefore a malfunction could occur*
- *failure detected by TSF according to FPT_TST.1*[77].

**Refinement:** The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

**Application Note 19:** Secure state called security reset for TOE.

**FPT_PHP.3 Resistance to Physical Attack**

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[78] to the *TSF*[79] by responding automatically such that the SFRs are always enforced.

**Application Note 20:** The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent

69 [assignment: types of emissions]
70 [assignment: specified limits]
71 [assignment: list of types of TSF data]
72 [assignment: list of types of user data]
73 [assignment: type of users]
74 [assignment: type of connection]
75 [assignment: list of type of TSF data]
76 [assignment: list of type of user data]
77 [assignment: list of types of failures in the TSF]
78 [assignment: physical tampering scenarios]
79 [assignment: list of TSF devices/elements]

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.

**FPT_TST.1 TSF Testing**

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, at the conditions *that critical commands are sent to the TOE*[80] to demonstrate the correct operation of the TSF[81].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF Data[82].

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

**Application Note 21:** Since the MRTD's chip uses state of the art smart card technology, it runs some self tests (for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3) at the request of the authorized user and some self tests (to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 "Operational Use") automatically.

## 6.3 SECURITY FUNCTIONAL REQUIREMENTS FOR ACTIVE AUTHENTICATION ONLY

**FIA_API.1/AA Authentication Proof of Identity – Active Authentication**

FIA_API.1.1/AA The TSF shall provide Active Authentication mechanism[83] to prove the identity of the TOE[84].

**Application Note 22:** The TOE signs the challenge sent by the terminal with the Active Authentication Private Key and then the terminal verifies the identity of eMRTD with the Active Authentication Public Key.

**FCS_COP.1/SIG_MRTD Cryptographic operation**

FCS_COP.1.1/SIG_MRTD The TSF shall perform *digital signature creation*[85] in accordance with a specified cryptographic algorithm *RSA CRT with SHA-1, SHA-256, SHA-384*

80 [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test shall occur]]
81 [selection: [assignment: parts of TSF], the TSF]
82 [selection: [assignment: parts of TSF data], TSF data]
83 [assignment: authentication mechanism]
84 [assignment: authorized user or role]
85 [assignment: list of cryptographic operations]

*or SHA-512 or ECDSA with SHA1, SHA-224, SHA-256, SHA-384 or SHA-512*[86]

and cryptographic key sizes

- *1024 to 2048 bits for RSA,*
- *192 to 521 bits for ECDSA*[87],

that meet the following: *scheme 1 of [ 20 ] for RSA, [ 17 ][ 18 ][ 19 ] for ECC*[88].

## 6.4 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures),

86 [assignment: cryptographic algorithm]
87 [assignment: cryptographic key sizes]
88 [assignment: list of standards]

## 6.5 SECURITY REQUIREMENTS DEPENDENCIES

### 6.5.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

The dependence of security functional requirements for Embedded OS and the security functional requirements are defined in the following Table.

**Table 10: Dependency of Composite TOE SFRs**

| # | Security Functional Requirement | Dependencies | Fulfilled by security requirements in this ST |
|---|---|---|---|
| 1. | FAU_SAS.1 | None | ---- |
| 2. | FCS_CKM.1 | --- FCS_CKM.2 or FCS_COP.1<br>--- FCS_CKM.4 | --- FCS_COP.1/ENC, FCS_COP.1/MAC<br>--- FCS_CKM.4 |
| 3. | FCS_CKM.4 | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | ---- FCS_CKM.1 |
| 4. | FCS_COP.1/SHA | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>--- FCS_CKM.4 | --- Not fulfilled but justified. See Explanation 1<br>--- Not fulfilled but justified. See Explanation 1 |
| 5. | FCS_COP.1/ENC | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>--- FCS_CKM.4 | --- FCS_CKM.1<br>--- FCS_CKM.4 |
| 6. | FCS_COP.1/AUTH | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>--- FCS_CKM.4 | --- Not fulfilled but justified. See Explanation 2<br>--- Not fulfilled but justified. See Explanation 2 |
| 7. | FCS_COP.1/MAC | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>--- FCS_CKM.4 | --- FCS_CKM.1<br>--- FCS_CKM.4 |
| 8. | FCS_RND.1 | None | ---- |
| 9. | FCS_COP.1/SIG_MRTD | --- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | --- Not fulfilled but justified. See Explanation 5 |

| # | Security Functional Requirement | Dependencies | Fulfilled by security requirements in this ST |
|---|---|---|---|
| | | --- FCS_CKM.4 | --- Not fulfilled but justified. See Explanation 5 |
| 10. | FIA_UID.1 | None | ---- |
| 11. | FIA_UAU.1 | --- FIA_UID.1 | --- FIA_UID.1 |
| 12. | FIA_UAU.4 | None | ---- |
| 13. | FIA_UAU.5 | None | ---- |
| 14. | FIA_UAU.6 | None | ---- |
| 15. | FIA_API.1/AA | None | ---- |
| 16. | FIA_AFL.1 | --- FIA_UAU.1 | --- FIA_UAU.1 |
| 17. | FDP_ACC.1 | --- FDP_ACF.1 | --- FDP_ACF.1 |
| 18. | FDP_ACF.1 | --- FDP_ACC.1<br>--- FDP_MSA.3 | --- FDP_ACC.1<br>--- Not fulfilled but justified. See Explanation 3 |
| 19. | FDP_UCT.1 | --- FTP_ITC.1 or FTP_TRP.1<br>--- FDP_ACC.1 or FDP_IFC.1 | --- Not fulfilled but justified. See Explanation 4<br>--- FDP_ACC.1 |
| 20. | FDP_UIT.1 | --- FDP_ACC.1 or FDP_IFC.1<br>--- FTP_ITC.1 or FTP_TRP.1 | --- FDP_ACC.1<br>--- Not fulfilled but justified. See Explanation 4 |
| 21. | FMT_SMF.1 | None | ---- |
| 22. | FMT_SMR.1 | --- FIA_UID.1 | --- FIA_UID.1 |
| 23. | FMT_LIM.1 | --- FMT_LIM.2 | --- FMT_LIM.2 |
| 24. | FMT_LIM.2 | --- FMT_LIM.1 | --- FMT_LIM.1 |
| 25. | FMT_MTD.1/INI_ENA | --- FMT_SMR.1 | --- FMT_SMR.1 |

| # | Security Functional Requirement | Dependencies | Fulfilled by security requirements in this ST |
|---|---|---|---|
| | | --- FMT_SMF.1 | --- FMT_SMF.1 |
| 26. | FMT_MTD.1/INI_DIS | --- FMT_SMR.1<br>--- FMT_SMF.1 | --- FMT_SMR.1<br>--- FMT_SMF.1 |
| 27. | FMT_MTD.1/KEY_WRITE | --- FMT_SMR.1<br>--- FMT_SMF.1 | --- FMT_SMR.1<br>--- FMT_SMF.1 |
| 28. | FMT_MTD.1/KEY_READ | --- FMT_SMR.1<br>--- FMT_SMF.1 | --- FMT_SMR.1<br>--- FMT_SMF.1 |
| 29. | FPT_EMSEC.1 | None | ---- |
| 30. | FPT_FLS.1 | None | ---- |
| 31. | FPT_PHP.3 | None | ---- |
| 32. | FPT_TST.1 | None | ---- |

**Explanation 1:** A key does not exist here since a hash function does not use key(s).

**Explanation 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, either.

**Explanation 3:** The access control TSF according to FDP_ACF.1 uses security attributes having been defined during the manufacturing and fixed over the whole life time of the TOE. No management of these security attributes (i.e., FMT_MSA.3) is necessary here.

**Explanation 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.

**Explanation 5:** The SFR FCS_COP.1/SIG_MRTD uses the asymmetric key permanently stored during the Personalization process. Since the key is permanently stored within the TOE, there is no need for FCS_CKM.1 and FCS_CKM.4

### 6.5.2 SECURITY ASSURANCE REQUIREMENTS DEPENDENCIES

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 a moderate to high level of independently assured security in conventional commodity TOEs are required.

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.

## 6.6 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The coverage of the TOE Security Objectives by the SFRs is given in Table 11. The rationale behind this coverage is also given in this section.

**Table 11: Coverage of TOE Objectives by SFRs**

| Security Functional Requirement | 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 | OT.Chip_Authenticity |
|---|---|---|---|---|---|---|---|---|---|
| FAU_SAS.1 | | | | ✓ | | | | | |
| FCS_CKM.1 | ✓ | ✓ | ✓ | | | | | | |
| FCS_CKM.4 | ✓ | | ✓ | | | | | | |
| FCS_COP.1/SHA | ✓ | ✓ | ✓ | | | | | | ✓ |
| FCS_COP.1/ENC | ✓ | ✓ | ✓ | | | | | | |
| FCS_COP.1/AUTH | ✓ | ✓ | | | | | | | |
| FCS_COP.1/MAC | ✓ | ✓ | ✓ | | | | | | |
| FCS_COP.1/SIG_MRTD | | | | | | | | | ✓ |
| FCS_RND.1 | ✓ | ✓ | ✓ | | | | | | |
| FIA_UID.1 | | | ✓ | ✓ | | | | | |
| FIA_AFL.1 | | | ✓ | ✓ | | | | | |

| Security Functional Requirement | 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 | OT.Chip_Authenticity |
|---|---|---|---|---|---|---|---|---|---|
| FIA_UAU.1 | | | ✓ | ✓ | | | | | |
| FIA_UAU.4 | ✓ | ✓ | ✓ | | | | | | |
| FIA_UAU.5 | ✓ | ✓ | ✓ | | | | | | |
| FIA_UAU.6 | ✓ | ✓ | ✓ | | | | | | |
| FIA_API.1/AA | | | | | | | | | ✓ |
| 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 | ✓ | ✓ | ✓ | | | | | | |
| FMT_MTD.1/KEY_READ | ✓ | ✓ | ✓ | | | | | | |
| FPT_EMSEC.1 | ✓ | | | | ✓ | | | | |
| FPT_TST.1 | | | | | ✓ | | ✓ | | |
| FPT_FLS.1 | ✓ | | | | ✓ | | ✓ | | |
| FPT_PHP.3 | ✓ | | | | ✓ | ✓ | | | |

**OT.AC_Pers:**

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 is 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 SFR FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

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 either by using the BAC mechanism (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) with the personalization key or for reasons of interoperability with the [ 3 ] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

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 Active Authentication Private Key and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

**OT.Data_Int:**

The security objective OT.Data_Int "Integrity of personal data" requires the TOE to protect the integrity of the logical 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 Initialization and Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using 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, for ENC_MAC_Mode, 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. 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.

**OT.Data_Conf:**

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 successfully authenticated Personalization Agent is allowed to read the data of the logical MRTD. The successfully authenticated Basic Inspection System is allowed to read the data of the logical MRTD specified in EF.COM. 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).

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 that 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.

**OT.Identification:**

The security objective OT.Identification "Identification and Authentication of the TOE" addresses 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 successfully authenticated Basic Inspection System 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 FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

**OT.Prot_Inf_Leak:**

The security objective OT.Prot_Inf_Leak "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure o 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 o by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

**OT.Prot_Phys-Tamper:**

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

**OT.Prot_Malfunction:**

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

**OT.Prot_Abuse-Func:**

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

**OT.Chip_Authenticity:**

The security objective OT.Chip_Authenticity "Protection against forgery" is ensured by the Active Authentication Protocol provided by FIA_API.1/AA, proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/SIG_MRTD and FCS_COP.1/SHA. It is performed using

a TOE internally stored confidential private key as required by FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ.

## 6.7 SECURITY ASSURANCE REQUIREMENTS RATIONALE

An assurance level of EAL4 with the augmentations ALC_DVS.2 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators shall have access to the detailed design knowledge and source code.

# 7 TOE SUMMARY SPECIFICATION

Security Features of the AKIS GEZGIN composite product are given below. Some of the security features are provided mainly by Security IC and others are mainly provided by the Embedded Software.

## 7.1 SF_PP: PHYSICAL PROTECTION

SF_PP, Physical Protection is mainly inherited from the Security IC part of composite product to AKIS GEZGIN. The Security Features of the Security IC Platform is SF_PS: Protection Against Snooping, SF_PMA: Protection Against Modification Attacks, SF_PLA: Protection Against Logical Attacks. For the detailed information Security IC ST [ 5 ] can be checked. In addition, the SFR FPT_EMSEC.1 is included as a requirement for the ES part of the composite product and some Error Detection Code Control based features are added to the Embedded Software for FPT_PHP.3 requirement to enhance the protection of the access control files.

Covered SFRs are FPT_PHP.3, FPT_FLS.1, FPT_TST.1 and FPT_EMSEC.1.

## 7.2 SF_DPM: DEVICE PHASE MANAGEMENT

Device phase management security feature is fulfilled by Security IC part of the composite product and the Embedded Software. For security features fulfilled by Security IC, please see the Security IC ST [ 5 ].

Covered SFRs are FAU_SAS.1, FMT_LIM.1, FMT_LIM.2.

## 7.3 SF_AC: ACCESS CONTROL

The TOE provides Access Control mechanisms with SF_AC that allow to maintain different users and to associate users with roles Manufacturer, Personalization Agent, Basic Inspection System.

**Manufacturer** is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

The TOE restricts to write the initialization and personalization keys to the **Manufacturer**. Once these keys are written, the **Personalization Agent** has rights to change both keys. No other roles are allowed to write or change these keys. The **Personalization Agent** has the rights to create files and keys and to read files and public keys in the Initialization and Personalization Phases correspondingly.

The **Personalization Agent** is the only role with the ability:

- to enable/disable read access for users to the Initialization Data,
- to write the Document Basic Access Keys,
- to write and to read the data of the EF.COM, EF.SOD, EF.DGs of the logical MRTD after successful authentication.

The TOE enforces access control on terminals by requiring authentication in the appropriate life cycle prior to gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG's of the logical MRTD.

The **Basic Inspection System**

- is allowed to read the data in EF.COM, EF.SOD, standard data in EF.DG1 to EF.DG16 of the logical MRTD after successful authentication,
- is not allowed to read the biometric data (e.g., data in EF.DG3 and EF.DG4) of the logical MRTD.

No terminal is allowed

- to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
- to read any of the EF.DG1 to EF.DG16 of the logical MRTD without authentication.

The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys and the Personalization Agent Keys.

Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

Therefore, the SFRs FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ are covered with Access Control Security feature.

## 7.4 SF_SM: SECURE MESSAGING

The TOE has SF.SM which allows the TOE to communicate to the external world securely. Secure Messaging feature protects the confidentiality and integrity of the messages going between the TOE and the Basic Inspection system.

After a successful BAC authentication, a secure channel is established based on Triple DES algorithm.

This security functionality ensures

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

If an error occurs in the secure messaging layer, the session keys are destroyed. Specifically, the channel will be closed in case of a received message with:

- inconsistent or missing MAC,
- wrong sequence counter,
- inconsistent TLV structure,
- plain access.

Therefore, covered SFRs are: FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FDP_UCT.1, FDP_UIT.1, and FCS_RND.1.

## 7.5 SF_IA: IDENTIFICATION AND AUTHENTICATION

After activation or reset of the TOE, no user is authenticated. TSF mediated actions on behalf of a user require the user's prior successful identification and authentication. The TOE supports user authentication by the following means:

- Basic Access Control Authentication Mechanism,
- Symmetric Authentication Mechanism based on Triple DES,
- Active Authentication

The Basic Inspection System authenticates to the TOE by means of Basic Access Control Authentication Mechanism with the Document Basic Access Keys. The Personalization Agent authenticates himself to the TOE by use of the Personalization Agent Keys with the Symmetric Authentication Mechanism. The TOE prevents reuse of authentication data related to the Basic Access Control Authentication Mechanism and the Symmetric Authentication Mechanism. After successful authentication of the terminal with Basic Access Control Authentication Mechanism, the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user. Protection of user data transmitted from the TOE to the terminal is achieved by means of secure messaging with encryption and message authentication codes once successful authentication of terminal with the Basic Access Control

Authentication Mechanism has been completed. After authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay errors.

In addition, Active Authentication security functionality ensures the Active Authentication is performed as described in [ 10 ] and [ 11 ] (if it is activated by the personalization agent).

Therefore, the SFRs FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_API.1/AA, FCS_COP.1/SIG_MRTD, FCS_COP.1/AUTH, FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ are covered.

## 7.6 SECURITY FUNCTIONS RATIONALE

Table 12 shows the assignment of security functional requirements to TOE's security functionality.

**Table 12: Coverage of SFRs by TOE Security Features**

| Security Functional Requirement | SF_PP | SF_DPM | SF_AC | SF_SM | SF_IA |
|---|---|---|---|---|---|
| FAU_SAS.1 | | ✓ | | | |
| FCS_CKM.1 | | | | ✓ | |
| FCS_CKM.4 | | | | ✓ | |
| FCS_COP.1/SHA | | | | ✓ | |
| FCS_COP.1/ENC | | | | ✓ | |
| FCS_COP.1/AUTH | | | | | ✓ |
| FCS_COP.1/MAC | | | | ✓ | |
| FCS_COP.1/SIG-MRTD | | | | | ✓ |
| FCS_RND.1 | | | | ✓ | |
| FIA_UID.1 | | | | | ✓ |
| FIA_AFL.1 | | | | | ✓ |
| FIA_UAU.1 | | | | | ✓ |
| FIA_UAU.4 | | | | | ✓ |
| FIA_UAU.5 | | | | | ✓ |
| FIA_UAU.6 | | | | | ✓ |
| FIA_API.1/AA | | | | | ✓ |
| FDP_ACC.1 | | | ✓ | | |

| Security Functional Requirement | SF_PP | SF_DPM | SF_AC | SF_SM | SF_IA |
|---|---|---|---|---|---|
| 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 | | | ✓ | | |
| FMT_MTD.1/KEY_READ | | | ✓ | | |
| FPT_EMSEC.1 | ✓ | | | | |
| FPT_TST.1 | ✓ | | | | |
| FPT_FLS.1 | ✓ | | | | |
| FPT_PHP.3 | ✓ | | | | |

# 8 ABBREVIATIONS AND DEFINITIONS

AA: Active Authentication

AES: Advanced Encryption Standard

AKİS: Akıllı Kart İşletim Sistemi (Smart Card Operating System)

APDU: Application Protocol Data Unit

BAC: Basic Access Control

BIS: Basic Inspection System

BIS-PACE: Basic Inspection System with PACE

CPU: Central Processing Unit

DES: Data Encryption Standard

DF: Dedicated File

DFA: Differential Fault Analysis

DPA: Differential Power Analysis

EAL: Evaluation Assurance Level

EAC: Extended Access Control

ECC: Elliptic Curve Cryptography

EF: Elementary File

EEPROM: Electrically Erasable Programmable Read Only Memory

EIS: Extended Inspection System

ES: Embedded Operating System

GIS: General Inspection System

IC: Integrated Circuit

ICAO: International Civil Aviation Organization

MF: Master File

MRZ: Machine Readable Zone

OSP: Organizational Security Policy

PA: Passive Authentication

PACE: Password Authenticated Connection Establishment

PP: Protection Profile

PTG.2: A class that defines the requirements for RNGs used in key generation, padding bit generation, etc. PTG.2 is defined AIS31 [ 36 ]

RAM: Random Access Memory

RSA: Ron Rivest, Adi Shamir and Leonard Adleman

ROM: Read Only Memory

SAC: Supplemental Access Control

SAR: Security Assurance Requirements

SHA: Secure Hash Algorithm

SPA: Simple Power Analysis

SFR: Security Functional Requirement

ST: Security Target

TPDU: Transmission Protocol Data Unit

TOE: Target of Evaluation

# 9 REFERENCES

[ 1 ] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035.

[ 2 ] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access control, Version 1.10, 25th March. 2009, BSI-PP-0055.

[ 3 ] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended access control, Version 1.10, 25th March. 2009, BSI-PP-0056.

[ 4 ] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 02.11.2011 BSI-CC-PP-0068-V2-2011.

[ 5 ] Security Target Lite M7892 B11 Recertification Including Optional Software Libraries RSA – EC – SHA2 – Toolbox; Common Criteria CCv3.1 EAL6 Augmented (EAL6+) Resistance to Attackers with High Attack Potential; Version 0.3, 2015-10-13.

[ 6 ] Common Criteria for Information Technology Security Evaluation Part I: Introduction and General Model; Version 3.1 Revision 4 CCMB-2012-09-001.

[ 7 ] Common Criteria for Information Technology Security Evaluation Part II: Security Functional Requirements; Version 3.1 Revision 4 CCMB-2012-09-002.

[ 8 ] Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 3.1 Revision 4 CCMB-2012-09-003.

[ 9 ] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, CCMB-2012-09-004.

**MRTD specifications**

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

[ 11 ] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization.

[ 12 ] Development of a logical data structure – LDS for optional capacity expansion technologies Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision – 1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18.

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

[ 14 ] Annex to Section III Security Standards for Machine Readable Travel Documents Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003.

[ 15 ] Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 3: Common Specifications, Version 2.10, 10 March 2012.

**Standards**

[ 16 ] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006 73 FQR 110 5767 Ed2.

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

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

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

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

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

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

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

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

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

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

[ 27 ] FIPS 46-3 Data Encryption Standard (DES). Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

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

[ 29 ] FIPS 197 – Advance Encryption Standard (AES).

[ 30 ] ISO 1177 - Information Processing Character Structure For Start/Stop And Synchronous Character Oriented Transmission, 1985-07-25.

[ 31 ] ISO 14443-3 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 3: Initialization and anticollision.

[ 32 ] ISO 14443-4 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 4: Transmission protocol.

[ 33 ] ISO 7816-4 Information Technology – Identification Cards – Integrated Circuits with Contacts, Part 4: Organization, security and commands for interchange, April, 2013.

[ 34 ] ISO 7816-8 Information Technology – Identification Cards – Integrated Circuits with Contacts, Part 8: Commands for security operations, Sep., 2009.

[ 35 ] ISO 7816-9 Information Technology – Identification Cards – Integrated Circuits with Contacts, Part 9: Commands for card management, Sep., 2009.

**Misc**

[ 36 ] Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik respectively —A proposal for: Functionality classes for random number generators , Version 2.0, 2011-09-18, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik