TÜBİTAK BİLGEM UEKAE

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

e-ID Technologies Unit

SECURITY TARGET LITE

of

AKIS GEZGIN_N v2.0

BAC Configuration and BAP Configuration 1

with Active Authentication

Revision no	01
Revision date	16.02.2024
Document code	AKiS-GEZGiN_N-BAC-BAP1-AA-ST-Lite-01
Prepared by	Ali YILDIRIM

REVISION HISTORY

Revision	Description	Date
1.	First public version of the ST created	16.02.2024

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: Security Target Lite of AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication

Document Version: 01

CC Version: 3.1 (Revision 5)

Assurance Level: EAL 4+ (augmented with ALC_DVS.2)

1.2 TOE REFERENCE

The current Security Target refers to the product AKIS GEZGIN_N BAC Configuration and BAP Configuration 1 with Active Authentication. The short version number of the TOE is 2.0 and the full version number of the TOE is 2.0.0.7.

1.3 TOE OVERVIEW

The Target of Evaluation (TOE) addressed by this security target is AKIS GEZGIN_N BAC Configuration and BAP Configuration 1 with Active Authentication. The TOE is the composition of contactless smartcard IC which is P71D352P of NXP N7121 P71D321 platform, platform crypto library, and the Embedded Operating System (EOS) supporting electronic Machine Readable Travel Document (eMRTD) application and ISO-compliant Driving Licence (IDL) application. The aim of this security target is to define the security assurance and functional requirements of the TOE.

In this document, both the terms “AKIS GEZGIN” and “AKIS GEZGIN_N” refer to “AKIS GEZGIN_N supporting Basic Access Control (BAC), Basic Access Protection (BAP) Configuration 1, and Active Authentication”.

The TOE comprises the following:

- the circuitry of the eMRTD’s (or IDL’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 / IDL application,
- activation data,
- guidance documentation with personalization recommendations.

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/IDL application. The composite product conforms to eMRTD specifications (AA, BAC, SAC and EAC) as well as IDL specifications (AA, BAP Configuration 1, SAC and EAC). The TOE is designed and developed to include an e-Passport (eMRTD) application and an ISO-compliant Driving Licence (IDL) application (eMRTD and IDL applications are mutually exclusive, i.e., the TOE cannot be personalized to include both applications). Personalization Agent selects the security features to be configured in the TOE depending on the governmental policies.

Supporting eMRTD and IDL, the TOE is a native software embedded in contactless smart card IC P71D352P of NXP N7121 P71D321 platform. During the manufacturing and personalization phases, the TOE can be configured to serve two different use cases: eMRTD and IDL.

The TOE provides five standard authentication protocols: In addition to Basic Access Control (BAC), Basic Access Protection (BAP) and Active Authentication (AA), the embedded software also implements Supplemental Access Control (SAC) and Extended Access Control (EAC). Only BAC and BAP configuration 1 along with Active Authentication (AA) are within the scope of this ST.

Part 3 of ISO-compliant driving licence (IDL) standard ISO 18013 [25] supports BAP configuration 1 instead of BAC. From a security point of view, BAP configuration 1 is identical to BAC in that encryption key and message authentication key used for BAP configuration 1 secure messaging are generated the same way that they are generated for BAC and that encryption and message authentication code calculation are the same as BAC. Therefore, BAP configuration 1 is also included within the scope of this ST.

Henceforth, since the TOE supports both eMRTD and IDL standards, the acronym for the term Machine Readable Document (MRD) will be used instead of MRTD and IDL, unless MRTD or IDL specifically mentioned.

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)	✓	✓[1]
Supplemental Access Control (SAC)	✓	X
Extended Access Control (EAC)	✓	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),
- Basic Access Protection (BAP),
- Hybrid Deterministic Random Number Generation,
- Signature generation with ISO 9796-2 Digital signature scheme 1,
- Signature generation with ECDSA.

1.3.3 NON-TOE HARDWARE/SOFTWARE/FIRMWARE REQUIRED BY THE TOE

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

1 BAP Configuration 1 only

1.4 TOE DESCRIPTION

1.4.1 LOGICAL SCOPE OF THE TOE

A logical TOE will have data of the TOE holder stored according to the Logical Data Structure as specified by ICAO Doc 9303 [10] for eMRTD and by ISO 18013-2 [24] for IDL on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the TOE holder.

- The digital MRZ[2] 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 § 1.3.2.

1.4.1.1 LDS APPLICATION

The Logical Data Structure (LDS) application is a generic file system that can be configured to meet ICAO Doc 9303 e-Passport specifications [10] or ISO 18013 ISO-compliant Driving Licence specifications [24].

The generic file system is given in Figure 1.

2 For eMRTD, MRZ is used for BAC protocol. For IDL, however, the SAI demarcates the input string which will be used for BAP Configuration 1. SAI content on IDL can be based on an existing text field, or can consist of a dedicated text field, barcode, or MRZ.

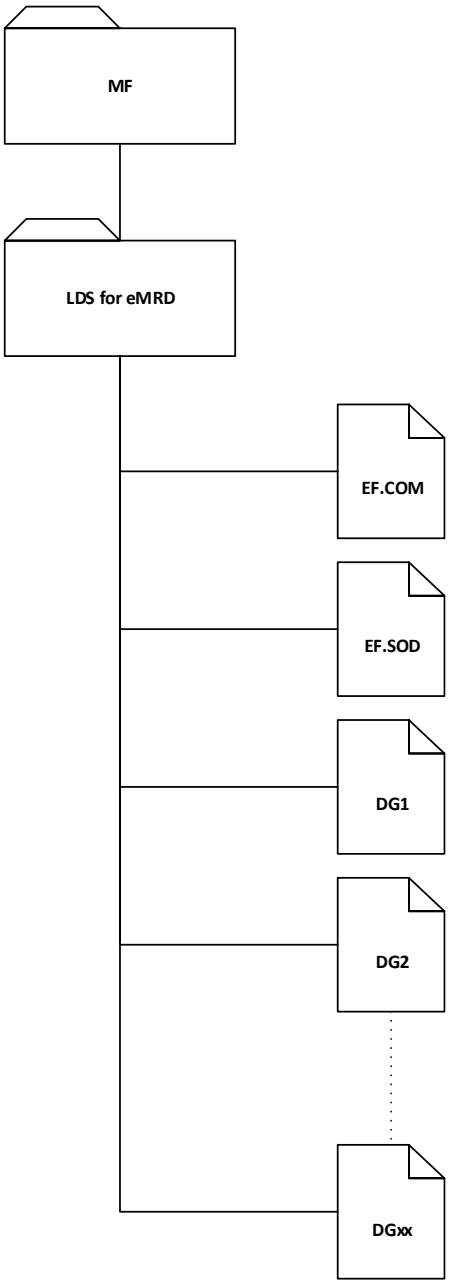


Figure 1: Generic file system of the TOE

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 which are located in the NVM area of the TOE. Access rights information, file size, file ID (FID) and short file identifier (SFI) are stored in the file header.

1.4.1.1.1 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. The system files used for MRD may be created and updated during the Personalization operation only. The keys stored in system 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/BAP.

1.4.1.1.2 DATA FILES

Data files also called Elementary files (EF) or Data Groups (DG) are dedicated to store data that may be retrieved. Data files may be created or updated during the Personalization phase and their integrity is protected by means of a checksum. The associated guidance documentation contains more detailed information about how and when these files may be created/updated.

Common data files for MRD are as follows:

- EF.COM which contains the list of DGs that 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,
- EF.DG1 up to EF.DG16 for eMRTD and EF.DG1 up to EF.DG14 for IDL containing information about the MRD holder (picture, name…) and key(s) required to perform authentications.

1.4.2 PHYSICAL SCOPE OF THE TOE

A physical TOE will be in form of a paper book or plastic card with an embedded chip and an antenna.

It presents visual readable data including (but not limited to) personal data of the MRD holder:

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

The antenna and the plastic or paper, optically readable, cover of the MRD, 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 which are 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 § 1.4.7 for more information on the IC platform.

The TOE comprises the following:

- the circuitry of the MRD's chip (contactless smartcard chip P71D352P of N7121 platform),
- the IC Dedicated Software with the parts IC Dedicated Test & Support Software and Symmetric Crypto Library
- the IC Embedded Software including operating system and eMRTD/IDL application,
- the guidance documentation with personalization recommendations.

All components of the TOE are listed in Table 2.

Table 2: Components of the TOE

Type	Name	Version	Form of Delivery
IC Hardware	N7121	B1	Wafer, modules and package
IC Dedicated Test Software	Test Software	9.2.3.0	On-chip software
IC Dedicated Support Software	Boot Software	9.2.3.0	On-chip software
	Firmware	9.2.3.0	On-chip software
	Library Interface	9.2.3.0	On-chip software
	Crypto Library	0.7.6	On-chip software
Security IC Embedded Software	AKIS GEZGIN_N	2.0	On-chip software
Document	AKIS GEZGIN_N v2.0 Yönetici ve Kullanıcı Kılavuzu	7	DOC or PDF via hand-delivery
Document	AKIS GEZGIN_N v2.0 Kişiselleştirme Kılavuzu	5	DOC or PDF via hand-delivery

Document	AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication Teslim ve İşletim Dokümanı	02	DOCX or PDF via hand-delivery
Activation data	N/A	N/A	Smartcard via hand-delivery or set of files via secure electronic delivery For details, see AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication Teslim ve İşletim Dokümanı

1.4.3 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 § 8,
- Passive Authentication (PA),
- Active Authentication (AA),
- Basic Access Control (BAC),
- Basic Access Protection (BAP),
- The following cryptographic operations for AA
    - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Operations,
    - Signature generation with ECDSA,
    - Signature generation with ISO 9796-2 Digital signature scheme 1,
    - Hybrid Deterministic Random Number Generation,
- The following cryptographic services for BAC and BAP Configuration 1
    - SHA-1,
    - DES3 Encryption and Decryption,
    - Retail MAC (DES3),
    - Hybrid Deterministic Random Number Generation.

Note that for Active Authentication, the hash operation SHA-1 is out of scope for the signature generation with ECDSA and SHA-224 is only used for the signature generation with ECDSA. Note also that the cryptographic operations SHA-1, SHA-224, SHA-256, SHA-384, SHA-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 hardware platform including the crypto library is certified for EAL 6 augmented and resistant to physical attacks. For details, please see the platform ST [5].

1.4.3.1 PASSIVE AUTHENTICATION (PA)

Passive Authentication (PA) ensures that the contents of the TOE are authentic and tamper-proof and have not changed since personalization. The TOE contains a file (SOD), located under the eMRTD/IDL application, which 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.

1.4.3.2 ACTIVE AUTHENTICATION (AA)

Active Authentication (AA) prevents cloning of MRD's chip. For this purpose, the 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, the TOE signs the data provided by the TOE environment therefore proving that the TOE contains the private component of the RSA or ECC key whose public component is already stored in data group EF.DG15 [3].

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

3 For IDL: EF.DG13

1.4.3.3 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.

1.4.3.4 BASIC ACCESS PROTECTION (BAP) CONFIGURATION 1

Basic Access Protection (BAP) is a mechanism used in e-driving licences 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 Scanning Area Identifier (SAI) of the TOE.

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

From a security point of view, BAP configuration 1 is identical to BAC in that encryption key and message authentication key used for BAP configuration 1 secure messaging are generated the same way that they are generated for BAC and that encryption and message authentication code calculation are the same as BAC.

1.4.4 INTERFACES

For the electrical I/O:

- ISO 1177 Information processing — Character structure for start/stop and synchronous character oriented transmission [18]
- ISO 14443-3 Cards and security devices for personal identification — Contactless proximity objects, Part 3: Initialization and anticollision [19]
- ISO 14443-4 Cards and security devices for personal identification — Contactless proximity objects, Part 4: Transmission protocol [20]

For the commands:

- ISO 7816 Commands [21], [22], [23]
- MRTD Commands [10]
- IDL commands [25]

1.4.5 LIFE CYCLE

This Security Target is based on the protection profile BSI-CC-PP-0055 and the life cycles of the composite product AKIS GEZGIN are based on the life cycles of this PP 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/IDL 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/IDL application and the guidance documentation is securely delivered to the MRD 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 MRD'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 MRD material during the IC manufacturing and the delivery process to the MRD manufacturer. The IC is securely delivered from the IC manufacturer to the MRD manufacturer.

- If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance NVM)[4].
- **(Step4)** The MRD manufacturer combines the IC with hardware for the contactless interface in the book/*card*.
- **(Step5)** The MRD manufacturer (i) creates the MRTD/IDL 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. The TOE accepts only PERFORM SECURITY OPERATION (PSO) command, activation command and some commands that provide very limited information about itself in this phase. When the TOE is sent the very first APDU, it checks the FabKey data: if the FabKey data does not match the expected value, the TOE enters the Death 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.*[5]
    - ***(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 MRD together with the IC Identifier is securely delivered from the MRD manufacturer to the Personalization Agent. The MRD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase-3: Personalization of the MRD

- **(Step6)** *This phase starts with the successful authentication of personalization key. Another successful authentication is needed to complete this phase. Personal information data are*

4 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.
5 Before activation, the IC embedded software can be removed from IC, for further version upgrades, by the MRD manufacturer using a cryptogram intended for flash loader activation only.

written and access rules are defined in this phase. Application specific restrictions cannot be implemented in personalization phase.

- The personalization of the MRD includes (i) the survey of the MRD holder's biographical data, (ii) the enrolment of the MRD 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 MRD, (iv) the writing of the TOE User Data and TSF Data into the logical MRD 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[6] data (EF.DG1), (ii) the digitized portrait (EF.DG2 [7]), and (iii) the Document security object.
- The signing of the Document security object by the Document Signer finalizes the personalization of the genuine MRD for the MRD holder. The personalized MRD (together with appropriate guidance for the TOE use if necessary) is handed over to the MRD holder for operational use.

Phase-4: Operational Use

- **(Step7)** The TOE is used as MRD's chip by the user and the inspection systems in the "Operational Use" phase. The user data on eMRD 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 or Organization but they can never be modified.

Phase-5: Death Phase

- *Death phase is defined by the 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.*

6 for eMRTD
7 For IDL: EF.DG4

1.4.6 TOE CONFIGURATIONS

AKIS GEZGIN_N BAC configuration and BAP Configuration 1 with Active Authentication is within the scope of this Security Target. The type of configuration is specified through writing to a special area in the NVM area during the Personalization Operation.

The TOE can be personalized for two types of applications: eMRTD and IDL. These applications are mutually exclusive, i.e., the TOE can be personalized to have only one of them.

1.4.7 PLATFORM INFORMATION

Platform:
NXP Technologies, N7121 P71D321

Platform ST:
NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, Rev. 2.6, 13 June 2022

Platform PP Conformance:
Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014

Platform Assurance Level:
EAL 6 augmented (ASE_TSS.2, ALC_FLR.1)

Platform Certification Report:
BSI-DSZ-CC-1136-V3-2022 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH

Common Criteria Version:
CC v3.1 Revision 5

2 CONFORMANCE CLAIM

2.1 CC CONFORMANCE CLAIM

This security target and the TOE claim conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.

as follows:

- Part 2 extended,
- Part 3 conformant.

2.2 PP CLAIM

This ST is based on BSI-CC-PP-0055, version 1.10, 25th March 2009 [2].
Since the TOE also supports the security mechanisms Active Authentication and Basic Access Protection (BAP) Configuration 1, new SFRs, in addition to those given in [2], are added to this ST.

2.3 PACKAGE CLAIM

The current ST is conformant to the following security requirements package: assurance package EAL 4 augmented with ALC_DVS.2 as defined in CC part 3 [8].

2.4 CONFORMANCE CLAIM RATIONALE

From a security point of view, BAP configuration 1 [25] is identical to BAC [11]; however, since (i) there does not exist a certified PP for BAP Configuration 1 and (ii) the types of TOE defined in this ST (please see §1.3.1) and PP-0055 [2] (please see §1.2) do not match, no strict conformance to a PP is claimed; instead, this ST is based on PP-0055.
An assurance level of EAL 4 with the augmentation ALC_DVS.2 is required for this type of TOE since it is intended to have the capability to defend against sophisticated attacks.

3 SECURITY PROBLEM DEFINITION

The security problem definition is based on the protection profile BSI-CC-PP-0055 which this ST is based on. 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/IDL 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/IDL APPLICATION

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

3.1.1.1 LOGICAL MRD 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 [10]. These are the 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.DG14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

The logical IDL data consists of the EF.COM, EF.DG1 to EF.DG14 (with different security needs) and the Document Security Object EF.SOD according to LDS [24]. These are the user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG11 contain personal data of the IDL holder. The Chip Authentication Public Key (EF.DG14) 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 IDL.

Due to interoperability reasons as stated in ICAO Doc 9303 [11] and ISO 18013-3 [25], the TOE described in this security target specifies only the BAC and BAP Configuration 1 mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRD standard User Data (i.e., Personal Data) of the MRD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, and EF.DG16 for eMRTD; EF.DG1 to EF.DG6 and EF.DG9 to EF.DG11 for IDL),
- Chip Authentication Public Key in EF.DG14,

- Active Authentication Public Key in EF.DG15 for eMRTD (EF.DG13 for IDL),
- 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 and EF.DG4 for eMRTD; EF.DG7 and EF.DG8 for IDL).

A sensitive asset is the following more general one.

3.1.1.2 AUTHENTICITY OF THE MRD'S CHIP

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

3.2 SUBJECTS AND EXTERNAL ENTITIES

This ST considers the subjects given in Table 3.

Table 3: Subjects and External Entities of the TOE

Subject	Definition
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the MRD Manufacturer completing the IC to the MRD's chip. The Manufacturer is the default user of the TOE during Phase 2 "Manufacturing". The TOE does not distinguish between the users IC Manufacturer and MRD Manufacturer using this role Manufacturer.
Personalization Agent	The agent is acting on behalf of the issuing State or Organization to personalize the MRD for the holder by some or all of the following activities: (i) establishing the identity the holder for the biographic data in the MRD, (ii) enrolling the biometric reference data of the MRD 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 MRD 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] for eMRTD ([25] for IDL).

Subject	Definition
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface.
Inspection system (IS)	A technical system used by the control officer[8] of the receiving State or Organization (i) examining an MRD presented by the user and verifying its authenticity and (ii) verifying the traveler as the MRD holder. The Basic Inspection System (BIS) : • contains a terminal for the contactless communication with the MRD's chip, • implements the terminals part of the BAC/BAP and/or AA Mechanisms, • gets the authorization to read the logical MRD under the Basic Access Control (or Basic Access Protection) by optical reading the MRD or other parts of the book/card providing this information. The General Inspection System (GIS)[9]: GIS is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS): In addition to the General Inspection System, EIS • implements the Terminal Authentication Protocol and • is authorized by the issuing State or Organization through the Document Verifier of the receiving State or Organization to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.
MRD Holder	The rightful holder of the MRD for whom the MRD is personalized by the issuing State or Organization.

8 A border control officer of the receiving State or Organization who has got the authority to inspect eMRTD is the control officer whereas an official of the receiving Organization who has got the authority to inspect IDL is the control officer.
9 This security target does not distinguish between the BIS, GIS and EIS because the Extended Access Control is out of scope.

Subject	Definition
Traveler	Person presenting the MRD to the inspection system and claiming the identity of the MRD holder.
Attacker[10]	A threat agent trying (i) to identify and to trace the movement of the MRD's chip remotely (i.e., without knowing or optically reading the printed MRZ/SAI), (ii) to read or to manipulate the logical MRD without authorization, or (iii) to forge a genuine MRD.

3.3 THREATS

3.3.1 HARDWARE RELATED THREATS

Threats related to hardware are given in Table 4.

Table 4: Hardware related threats

No	Threat	Definition
1.	T.Phys-Tamper: Physical Tampering	**Adverse action:** An attacker may perform physical probing of the MRD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRD's chip Embedded Software. An attacker may physically modify the MRD's chip in order to (i) modify security features or functions of the MRD's chip, (ii) modify security functions of the MRD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g., the biometric reference data for the inspection system) or TSF Data (e.g., authentication key of the MRD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g., to enable information leakage

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

		through power analysis). Physical tampering requires direct interaction with the MRD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary. **Threat agent:** having enhanced basic attack potential, being in possession of a legitimate MRD. **Asset:** confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.
2.	T.Information_Leakage: Information Leakage from the MRD's chip	**Adverse action:** An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g., Differential Fault Analysis). **Threat agent:** having enhanced basic attack potential, being in possession of a legitimate MRD. **Asset:** confidentiality of logical MRD and TSF data

3.	T.Malfunction: Malfunction due to Environmental Stress	**Adverse action:** An attacker may cause a malfunction of TSF or of the MRD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRD's chip Embedded Software. This may be achieved, e.g., by operating the chip outside the normal operating conditions, exploiting errors in the MRD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation. **Threat agent:** having enhanced basic attack potential, being in possession of a legitimate MRD **Asset:** confidentiality and authenticity of logical MRD 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 Phase 4 "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRD holder. **Threat agent:** having enhanced basic attack potential, being in possession of a legitimate MRD. **Asset:** confidentiality and authenticity of logical MRD and TSF data, correctness of TSF.
5.	T.Counterfeit: Production of unauthorized copies or reproductions of	**Adverse action:** An attacker produces an unauthorized copy or reproduction of a genuine MRD's chip to be used as the chip of a counterfeit MRD. The attacker may either (i) generate a new data set from scratch or (ii) extract completely or partially the data from a genuine MRD's chip and then copy them on another chip to imitate the genuine MRD's chip.

	genuine MRD's chips	**Threat agent:** having high attack potential, being in possession of one or more legitimate MRDs and blank MRDs. **Asset:** authenticity of the MRD's chip

3.3.2 TERMINAL, COMMUNICATION AND APPLICATION RELATED THREATS

Terminal, communication and application related threats are given in Table 5.

Table 5: Application related threats

No	Threat	Definition
1.	T.Chip_ID: Identification of MRD's chip	**Adverse action:** An attacker trying to trace the movement of the MRD by identifying remotely the MRD's chip by establishing or listening to communications through the contactless communication interface. **Threat agent:** having enhanced basic attack potential, not knowing the optically readable MRZ/SAI data printed on the MRD data page in advance. **Asset:** Anonymity of user.
2.	T.Skimming: Skimming the logical MRD	**Adverse action:** An attacker imitates an inspection system trying to establish a communication to read the logical MRD or parts of it via the contactless communication channel of the TOE. **Threat agent:** having enhanced basic attack potential, not knowing the optically readable MRZ/SAI data printed on the MRD data page in advance. **Asset:** confidentiality of logical MRD 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 MRD's chip and an inspection system to gain the logical MRD or parts of it. The inspection system uses the MRZ/SAI data printed on the MRD data page but the attacker does not know these data in advance. **Threat agent:** having enhanced basic attack potential, not knowing the optically readable MRZ/SAI data printed on the MRD in advance **Asset:** confidentiality of logical MRD data

4.	T.Forgery: Forgery of data on MRD's chip	**Adverse action:** An attacker alters fraudulently the complete stored logical MRD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRD forgery. The attacker may alter the biographical data on the biographical data page of the book/card, in the printed MRZ/SAI and in the digital MRZ[11] 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 MRDs to create a new forged MRD, e.g., the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRD of a traveler into another MRD's chip leaving their digital MRZ[12] unchanged to claim the identity of the holder this MRD. The attacker may also copy the complete unchanged logical MRD to another contactless chip. **Threat agent:** having enhanced basic attack potential, being in possession of one or more legitimate MRDs. **Asset:** authenticity of logical MRD data

11 for eMRTD
12 for eMRTD

3.4 ORGANISATIONAL SECURITY POLICIES

Organizational security policies of the composite TOE are given in Table 6.

Table 6: Composite TOE Policies

No	Policy	Definition
1.	P.Manufact: Manufacturing of the MRD's chip	The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.
2.	P.Personalization: Personalization of the MRD 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 MRD with respect to the MRD holder. The personalization of the MRD 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[13] and stored on MRD'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 MRD's chip are personal data of the MRD holder. These data groups are intended to be used only with agreement of the MRD holder by inspection systems to which the MRD is presented. The chip shall provide the possibility for the BAC/BAP 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], [25]. (Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.)

13 for eMRTD

3.5 ASSUMPTIONS

Assumptions for the operational environment of the composite TOE are given in Table 7.

Table 7: Composite TOE Assumptions

No	Assumption	Definition
1.	A.MRD_Manufact: MRD manufacturing on steps 4 to 6	It is assumed that appropriate functionality testing of the MRD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRD and of the manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
2.	A.MRD_Delivery: Delivery of the MRD during steps 4 to 6	Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives: - Procedures shall ensure protection of TOE material/information under delivery and storage. - Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage. - Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.
3.	A.Pers_Agent: Personalization of the MRD's chip	The Personalization Agent ensures the correctness of (i) the logical MRD with respect to the MRD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

No	Assumption	Definition
4.	A.Insp_Sys: Inspection Systems for global interoperability	The Inspection System is used by the control officer of the receiving State or Organization for eMRD (i) examining an MRD presented by the user and verifying its authenticity and (ii) verifying the traveler as the MRD 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] (or Basic Access Protection [25]). The Basic Inspection System reads the logical MRD under BAC/BAP and performs the Passive Authentication to verify the logical MRD.
5.	A.BAC-Keys: Cryptographic quality of BAC/BAP Keys	The Document BAC/BAP Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of ICAO Doc 9303 [11], the Document BAC Keys are derived from a defined subset of the individual printed MRZ data (accordingly, as a consequence of ISO 18013-3 [25], the Document BAP Keys are derived from a defined subset of the individual printed SAI 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/SAI data with enhanced basic attack potential.
6.	A.Pers_Agent_AA: Personalization of the MRD's chip including Active Authentication	The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15 for eMRTD and EF.DG13 for IDL) if stored on the MRD's chip.

No	Assumption	Definition
		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 which this ST is based on. Since the TOE also supports Active Authentication mechanism, 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 MRD [14]

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [10] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

In cases where the TOE is to be used as an IDL, the TOE must also ensure that the logical IDL data in EF.DG1 to EF.DG14, the Document security object according to LDS [24] and the TSF data can be written by authorized Personalization Agents only. The logical IDL data in EF.DG1 to EF.DG14 and the TSF data may be written only during and cannot be changed after its personalization. The Document

14 OT.AC_Pers implies that (1) the data of the LDS groups written during personalization for MRD 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.

security object can be updated by authorized Personalization Agents if data in the data groups EF.DG2 to EF.DG14 are added.

OT.Data_Int: Integrity of personal data

The TOE must ensure the integrity of the logical MRD stored on the MRD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRD data.

OT.Data_Conf: Confidentiality of personal data

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

In cases where the TOE is to be used as an IDL, the TOE must ensure the confidentiality of the logical IDL data groups EF.DG1 to EF.DG14. Read access to EF.DG1 to EF.DG14 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1 to EF.DG6 and EF.DG9 to EF.DG14 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Protection based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical IDL 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 non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRD". 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 TOE must provide means to check FabKey data when the very first APDU command is received in the lifetime of the TOE.
The TOE must also provide means to update the EOS, before it is activated, in non-volatile memory for which all the security requirements of the platform are fulfilled.
The following TOE security objectives address the protection provided by the MRD’s chip independent of the TOE environment.

OT.Prot_Abuse-Func: Protection against Abuse of Functionality

After delivery of the TOE to the MRD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, 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 MRD’s chip;

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

OT.Prot_Phys-Tamper: Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRD’s chip Embedded Software. This includes protection against attacks with 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 to verify the authenticity of the MRD'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

This section describes the security objectives for the operational environment of the TOE.

4.2.1 ISSUING STATE OR ORGANIZATION

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

OE.MRD_Manufact: Protection of the MRD 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.MRD_Delivery: Protection of the MRD delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,

- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
    - origin and shipment details,
    - reception, reception acknowledgement,
    - location material/information.

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

OE.Personalization: Personalization of logical MRD

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 MRD, (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 MRD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign: Authentication of logical MRD 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 MRD 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 [10]. For IDL, however, the digital signature in the Document Security Object relates all data in the data in EF.DG1 to EF.DG14 if stored in the LDS according to [24].

OE.BAC-Keys: Cryptographic quality of Basic Access Control / Basic Access Protection Keys

The Document Basic Access Control / Basic Access Protection Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength.

As a consequence of ICAO Doc 9303 [11], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data (accordingly, as a consequence of ISO 18013-3 [25], the Document Basic Access Protection keys are derived from a defined subset of the individual printed SAI 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/SAI 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 MRD's Active Authentication Key Pair,
- Sign and store the Active Authentication Public Key in EF.DG15 [15],
- Store the Active Authentication Private Key in secure memory,
- Support inspection systems of receiving States or Organizations to verify the authenticity of the MRD'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_MRD: Examination of the MRD book/card

The inspection system of the receiving State or Organization must examine the MRD presented by the user to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or

15 For IDL: EF.DG13

Organization, and (ii) implements the terminal part of the Basic Access Control [11] / Basic Access Protection [25].

OE.Passive_Auth_Verif: Verification by Passive Authentication

The control officer of the receiving State or Organization for eMRD uses the inspection system to verify the traveler as the MRD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRD before they are used. The receiving 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_MRD: Protection of data from the logical MRD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRD. The receiving State or Organization examining the logical MRD under BAC/BAP will use inspection systems which implement the terminal part of the BAC/BAP and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e., Basic Inspection Systems).

OE.Exam_MRD_AA: Examination of the MRD book/card using Active Authentication

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

4.3 SECURITY OBJECTIVES RATIONALE

The rationale between security objectives and threats, OSPs, and assumptions is given in Table 8.

Table 8: 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.MRD_Manufact	OE.MRD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Active_Auth_Key	OE.Exam_MRD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRD	OE.Exam_MRD_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.MRD_Manufact										X									
A.MRD_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 9: 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 MRD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions".
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 MRD and misuse of the functions for personalization in the operational state after delivery to holder to disclose or to manipulate the logical MRD. This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRD" ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRD 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 MRD movement by identifying remotely the MRD's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by BAC/BAP 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	

Threats / OSPs / Assumptions	Corresponding Objectives	Rationale
T.Eavesdropping	OT.Data_Conf	The threats **T.Skimming** "Skimming digital MRZ[16] data or the digital portrait" and **T.Eavesdropping** "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical MRD trough the contactless interface or listening the communication between the MRD's chip and a terminal. This threat is countered by the security objective **OT.Data_Conf** "Confidentiality of personal data" through BAC/BAP using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRD, OE.Passive_Auth_Verif	The threat **T.Forgery** "Forgery of data on MRD's chip" addresses the fraudulent alteration of the complete stored logical MRD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRD" requires the TOE to limit the write access for the logical MRD to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity of the stored logical MRD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The examination of the presented MRD book/card according to **OE.Exam_MRD** "Examination of the MRD book/card" shall ensure that MRD book/card does not contain a sensitive contactless chip which may present the complete unchanged logical MRD. The TOE environment will detect partly forged logical MRD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical MRD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".
T.Counterfeit	OT.Prot_Abuse-Func, OT.Prot_Inf_Leak,	The threat **T.Counterfeit** "Production of unauthorized copies or reproductions of genuine

16 for eMRTD

Threats / OSPs / Assumptions	Corresponding Objectives	Rationale
	OT.Prot_Phys-Tamper, OT.Prot_Malfunction, OT.Chip_Authenticity, OE.Exam_MRD_AA, and OE.Active_Auth_Key	MRD's chips" addresses the attack of generating unauthorized copies or reproductions of genuine MRD's chips. This attack is countered by a set of objectives that ensure MRD'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 eMRD supports Active Authentication, the TOE addresses extra protections against this threat by proving the authenticity of the MRD'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_MRD_AA** "Examination of the MRD book/card using Active Authentication" and **OE.Active_Auth_Key** "Active Authentication Key" all participate in the detection of counterfeit MRD's chip by the inspection system.
P.Manufact	OT.Identification	The OSP **P.Manufact** "Manufacturing of the MRD'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 MRD by issuing State or Organization only" addresses the (i) the enrolment of the logical MRD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRD", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRD". Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and management of TSF to the Personalization Agent.
P.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

Threats / OSPs / Assumptions	Corresponding Objectives	Rationale
		MRD by means of the BAC/BAP and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT.Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.
A.MRD_Manufact	OE.MRD_Manufact	The assumption **A.MRD_Manufact** "MRD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment **OE.MRD_Manufact** "Protection of the MRD Manufacturing" that requires to use security procedures during all manufacturing steps.
A.MRD_Delivery	OE.MRD_Delivery	The assumption **A.MRD_Delivery** "MRD delivery during step 4 to 6" is covered by the security objective for the TOE environment **OE.MRD_Delivery** "Protection of the MRD delivery" that requires to use security procedures during delivery steps of the MRD.
A.Pers_Agent	OE.Personalization	The assumption **A.Pers_Agent** "Personalization of the MRD's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRD" including the enrolment, the protection with digital signature and the storage of the MRD holder personal data.
A.Insp_Sys	OE.Exam_MRD, OE.Prot_Logical_MRD	The examination of the MRD 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_MRD** "Examination of the MRD book/card". The security objectives for the TOE environment **OE.Prot_Logical_MRD** "Protection of data from the logical MRD" will require the Basic Inspection System to implement the BAC/BAP and to protect the logical MRD 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/BAP Keys" ensuring

Threats / OSPs / Assumptions	Corresponding Objectives	Rationale
		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 MRD's chip including Active Authentication" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRD" including the protection with a digital signature (SOD signing), the storage of the MRD 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_MRD_AA	The examination of the MRD 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_MRD_AA** "Examination of the MRD book/card using Active Authentication" that requires the Basic Inspection System to implement and to enforce Active Authentication of the MRD as part of the MRD'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.

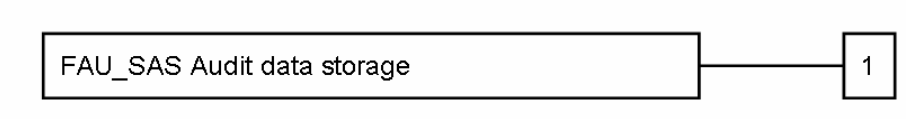
5.1 DEFINITION OF THE FAMILY FAU_SAS (AUDIT DATA STORAGE)

FAU_SAS family of the Class FAU (Security Audit) is defined in PP-0055 [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.

Dependencies: No dependencies.

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.

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

FCS_RND of the Class FCS (cryptographic support) is defined in PP-0055 [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 QUALITY METRIC FOR RANDOM NUMBERS

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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*].

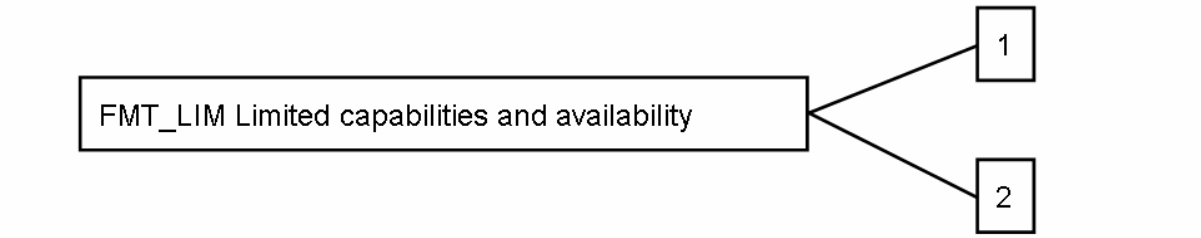
5.4 DEFINITION OF THE FAMILY FMT_LIM (Limited Capabilities and Availability)

FMT_LIM of the Class FMT (Security Management) is defined as given in PP-0055 [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.

Dependencies: FMT_LIM.2 Limited availability

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*].

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

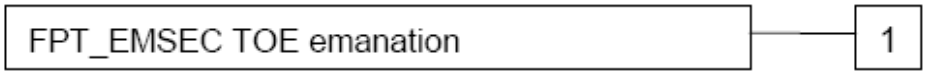
FPT_EMSEC (TOE emanation) of the Class FPT (Protection of the TSF) is defined as given in PP-0055 [2].

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 Part 2.

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 operations are defined in § 8.1 of Common Criteria Part 1 [6]. All these operations are 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 words are ~~crossed out~~.

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

The **assignment in a selection** operation is used when an assignment operation is selected from a list of selection options. Assignments in selections are denoted by *italicized and underlined text*.

Since this ST claims no conformance to any protection profiles, the CC functional requirements will be used here exactly as defined in CC Part 2 [7].

6.2 SECURITY FUNCTIONAL REQUIREMENTS

This ST is based on the protection profile BSI-CC-PP-0055 and all the SFRs in the PP are included in this ST. Since the TOE also supports Basic Access Protection and Active Authentication, the SFRs directly related to Basic Access Protection and Active Authentication are included here as well. In addition, the SFRs FDP_ACC.1 and FDP_ACF.1 are iterated for BAC and BAP.

TOE security functional requirements of the composite product are listed in Table 10.

Table 10: List of SFRs

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 – MRD
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_COP.1/SIG_MRD	Cryptographic operation – Signature generation for Active Authentication
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 – Re-authenticating of Terminal by the TOE
FIA_AFL.1	Authentication Failure Handling
FIA_API.1	Authentication Proof of Identity – Active Authentication
FDP_ACC.1/BAC	Subset access control – Basic Access Control
FDP_ACC.1/BAP	Subset access control – Basic Access Protection
FDP_ACF.1/BAC	Basic Security attribute based access control – Basic Access Control
FDP_ACF.1/BAP	Basic Security attribute based access control – Basic Access Protection
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

6.2.1 CLASS FAU: SECURITY AUDIT

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the *IC Manufacturer*[17] with the capability to store *the IC Identification Data*[18] 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

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Document Basic Access Key Derivation Algorithm*[19] and specified cryptographic key sizes *112 bits*[20] that meet the following *ICAO Doc 9303 [11] normative appendix 5 and ISO 18013-3 [25], Annex B (normative)*[21].

FCS_CKM.4 Cryptographic Key Destruction - MRD

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *secure erasing of the key value*[22] that meets the following: *none*[23].

17 [assignment: authorized users]
18 [assignment: list of audit information]
19 [assignment: cryptographic key generation algorithm]
20 [assignment: cryptographic key sizes]
21 [assignment: list of standards]
22 [assignment: cryptographic key destruction method]
23 [assignment: list of standards]

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform *hashing*[24] in accordance with a specified cryptographic algorithm *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512* [25] and cryptographic key sizes *none*[26] that meet the following: *U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4 [16], August 2015, section 6.2 SHA-256* [27].

Application Note 1: The hashing algorithm is defined by the personalization agent during the personalization. SHA-1 is a cryptographically weak hashing algorithm; however, since SHA-1 is included in ICAO Doc 9303 [11] and ISO 18013-3 [25] standards, it is included here as a result.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform *secure messaging (BAC/BAP) - encryption and decryption*[28] in accordance with a specified cryptographic algorithm *Triple DES in CBC Mode*[29] and cryptographic key sizes *112 bits*[30] that meet the following: *FIPS 46-3 [15], ICAO Doc 9303 [11], normative appendix 5, A5.3 and ISO 18013-3 [25], Annex B (normative), B.8* [31]**.**

24 [assignment: list of cryptographic operations]
25 [assignment: cryptographic algorithm]
26 [assignment: cryptographic key sizes]
27 [assignment: list of standards]
28 [assignment: list of cryptographic operations]
29 [assignment: cryptographic algorithm]
30 [assignment: cryptographic key sizes]
31 [assignment: list of standards]

FCS_COP.1/AUTH Cryptographic Operation - Authentication

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform *symmetric authentication - encryption and decryption*[32] in accordance with a specified cryptographic algorithm *AES in CBC mode*[33] and cryptographic key sizes *256 bits*[34] that meet the following: *FIPS 197 [17], NIST SP 800-38A [14]* [35]**.**

FCS_COP.1/MAC Cryptographic Operation - Retail MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform *secure messaging – message authentication code*[36] in accordance with a specified cryptographic algorithm *Retail MAC*[37] and cryptographic key sizes *112 bits*[38] that meet the following: *ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)* [39].

32 [assignment: list of cryptographic operations]
33 [assignment: cryptographic algorithm]
34 [assignment: cryptographic key sizes]
35 [assignment: list of standards]
36 [assignment: list of cryptographic operations]
37 [assignment: cryptographic algorithm]
38 [assignment: cryptographic key sizes]
39 [assignment: list of standards]

FCS_COP.1/SIG_MRD Cryptographic operation – Signature generation for Active Authentication

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG_MRD	The TSF shall perform *digital signature creation*[40] in accordance with a specified cryptographic algorithm *RSA CRT or ECDSA*[41] and cryptographic key sizes *1976 to 2560 bits for RSA and 224 to 521 bits for ECDSA*[42] that meet the following: *ISO 9796-2 Digital signature scheme 1 [13] for RSA, [12] for ECC*[43].

Application Note 2: The cryptographic functionality of the TOE includes signature generation with RSA keys of 1024-to-2560 bits and ECDSA signature generation with ECC keys of 128-to-640 bits. However, due to security considerations and BSI recommendations (see the security target of the platform), certification of the platform covers standard elliptic curves ansix9p224r1, ansix9p256r1, ansix9p384r1, ansix9p521r1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, and ANSSI FRP256v1. As a consequence, the certification of the TOE covers only these elliptic curves as well. In addition, RSA key lengths under 1976 bits are out of scope for the certification. The hash operation SHA-1 for signature generation with ECDSA is out of scope as well.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

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

DRG.4.1 The internal state of the RNG shall use PTRNG or class PTG.2 (as defined in [26]) as random source.

DRG.4.2 The RNG provides forward secrecy (as defined in [26]).

40 [assignment: list of cryptographic operations]
41 [assignment: cryptographic algorithm]
42 [assignment: cryptographic key sizes]
43 [assignment: list of standards]

DRG.4.3 The RNG provides backward secrecy even if the current internal state is known (as defined in [26]).

DRG.4.4 The RNG provides enhanced forward secrecy on demand (as defined in [26]).

DRG.4.5 The internal state of the RNG is seeded by an PTRNG or class PTG.2 (as defined in [26]).

DRG.4.6 The RNG generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least 1 - 2^{-24}.

DRG.4.7 Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [26]).

6.2.3 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_UID.1 Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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 MRD",*
- *to read the random identifier in Phase 4 "Operational Use"* [44]

on behalf of the user to be performed before the user is identified.

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

FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

- *to read the Initialization Data in Phase 2 "Manufacturing",*

44 [assignment: list of TSF-mediated actions]

- *to read the random identifier in Phase 3 "Personalization of the MRD",*
- *to read the random identifier in Phase 4 "Operational Use"* [45]

on behalf of the user to be performed before the user is authenticated.

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *Basic Access Control Authentication Mechanism,*
- *Basic Access Protection Configuration 1 Authentication Mechanism,*
- *Authentication mechanism based on AES*[46].

FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

- *Basic Access Control Authentication Mechanism,*
- *Basic Access Protection Configuration 1 Authentication Mechanism,*
- *Symmetric Authentication Mechanism based on AES* [47]

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 (or Basic Access*

45 [assignment: list of TSF mediated actions]
46 [assignment: identified authentication mechanism(s)]
47 [assignment: list of multiple authentication mechanisms]

Protection Configuration 1 Authentication Mechanism) with the Document Basic Access Keys[48].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions *each command sent to the TOE during a BAC (or BAP Configuration 1) mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism (or Basic Access Protection Configuration 1 Authentication Mechanism)* [49].

FIA_AFL.1 Authentication Failure Handling - BAC/BAP

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *1 to 10* [50] unsuccessful authentication attempts occur related to *BAC (or BAP Configuration 1) authentication protocol*[51].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[52], 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/BAP authentication attempts*[53].

FIA_API.1 Authentication Proof of Identity – Active Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide *Active Authentication mechanism*[54] to prove the identity of *the TOE*[55].

48 [assignment: rules describing how the multiple authentication mechanisms provide authentication]
49 [assignment: list of conditions under which re-authentication is required]
50 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
51 [assignment: list of authentication events]
52 [selection: met, surpassed]
53 [assignment: list of actions]
54 [assignment: authentication mechanism]
55 [assignment: authorized user or role]

6.2.4 CLASS FDP: USER DATA PROTECTION

FDP_ACC.1/BAC Subset access control – Basic Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/BAC The TSF shall enforce the *Basic access control SFP*[56] on *terminals gaining write, read and modification access to data in EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD*[57].

FDP_ACC.1/BAP Subset access control – Basic Access Protection

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/BAP The TSF shall enforce the *Basic access protection SFP*[58] on *terminals gaining write, read and modification access to data in EF.COM, EF.SOD, EF.DG1 to EF.DG14 of the logical IDL*[59].

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/BAC The TSF shall enforce the *Basic access control SFP*[60] to objects based on the following:

Subjects:

- *Personalization Agent,*
- *Basic Inspection System,*
- *Terminal,*

Objects:

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

56 [assignment: access control SFP]
57 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
58 [assignment: access control SFP]
59 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
60 [assignment: access control SFP]

- *data in EF.COM,*
- *data in EF.SOD,*

Security attributes:

- *authentication status of terminals*[61]*.*

FDP_ACF.1.2/BAC 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,*
- *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*[62]*.*

FDP_ACF.1.3/BAC The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[63]*.*

FDP_ACF.1.4/BAC The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- *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 of the logical MRTD*[64]*.*

61 [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]
62 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
63 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
64 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_ACF.1/BAP Basic Security attribute based access control – Basic Access Protection

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/BAP The TSF shall enforce the *Basic access protection SFP*[65] to objects based on the following:

Subjects:

- *Personalization Agent,*
- *Basic Inspection System,*
- *Terminal,*

Objects:

- *data EF.DG1 to EF.DG14 of the logical IDL,*
- *data in EF.COM,*
- *data in EF.SOD,*

Security attributes:

- *authentication status of terminals*[66]*.*

FDP_ACF.1.2/BAP 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.DG14 of the logical IDL,*
- *the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1 to EF.DG6 and EF.DG9 to EF.DG14 of the logical IDL*[67]*.*

65 [assignment: access control SFP]
66 [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]
67 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

FDP_ACF.1.3/BAP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[68].

FDP_ACF.1.4/BAP The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- *Any terminal is not allowed to modify any of the EF.DG1 to EF.DG14 of the logical IDL,*
- *Any terminal is not allowed to read any of the EF.DG1 to EF.DG14 of the logical IDL,*
- *The Basic Inspection System is not allowed to read the data in EF.DG7 and EF.DG8 of the logical IDL*[69].

FDP_UCT.1 Basic data exchange confidentiality - MRD

Hierarchical to: No other components.

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

FDP_UCT.1.1 The TSF shall enforce the *Basic access control SFP or Basic access protection SFP*[70] to transmit and receive[71] user data in a manner protected from unauthorized disclosure.

68 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
69 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
70 [assignment: access control SFP(s) and/or information flow control SFP(s)]
71 [selection: transmit, receive]

FDP_UIT.1 Data exchange integrity - MRD

Hierarchical to: No other components.

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

FDP_UIT.1.1 The TSF shall enforce the *Basic access control SFP or Basic access protection SFP*[72] to transmit and receive[73] user data in a manner protected from modification, deletion, insertion and replay[74] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[75] has occurred.

6.2.5 CLASS FMT: SECURITY MANAGEMENT

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

- *initialization,*
- *pre-personalization*
- *personalization*[76]*.*

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles

- *manufacturer,*
- *personalization agent,*

72 [assignment: access control SFP(s) and/or information flow control SFP(s)]
73 [selection: transmit, receive]
74 [selection: modification, deletion, insertion, replay]
75 [selection: modification, deletion, insertion, replay]
76 [assignment: list of management functions to be provided by the TSF]

- *basic inspection system*[77].

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

FMT_LIM.1 Limited Capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited Availability

FMT_LIM.1.1 The TSF shall be designed 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,*
- *software to be reconstructed and*
- *substantial information about construction of TSF to be gathered which may enable other attacks*[78].

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 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*[79].

77 [assignment: the authorised identified roles]
78 [assignment: Limited capability and availability policy]
79 [assignment: Limited capability and availability policy]

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to *write*[80] the *Initialization Data and Pre-Personalization Data*[81] to *the Manufacturer*[82].

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to *disable read access for users to*[83] the *Initialization Data*[84] to *the Personalization Agent*[85].

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles
FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to *write*[86] the *Document Basic Access keys and Active Authentication Private Key*[87] to *the Personalization Agent*[88].

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

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

80 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
81 [assignment: list of TSF data]
82 [assignment: the authorised identified roles]
83 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
84 [assignment: list of TSF data]
85 [assignment: the authorised identified roles]
86 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
87 [assignment: list of TSF data]
88 [assignment: the authorised identified roles]

	FMT_SMR.1 Security Roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to *read*[89] the *Document Basic Access Keys, Active Authentication Private Key and Personalization Agent Keys*[90] to *none*[91].

6.2.6 CLASS FPT: PROTECTION OF THE TSF

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMSEC.1.1 The TOE shall not emit *power variations, timing variations during command execution*[92] in excess of *non-useful information*[93] enabling access to *Personalization Agent Key, Active Authentication Private Key*[94] and *none*[95].

FPT_EMSEC.1.2 The TSF shall ensure *any unauthorized users*[96] are unable to use the following interface *smart card circuit contacts*[97] to gain access to *Personalization Agent Key and Active Authentication Private Key*[98] and *none*[99].

FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

Dependencies: No Dependencies.

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

- *exposure to out-of-range operating conditions where therefore a malfunction could occur*
- *failure detected by TSF according to FPT_TST.1* [100].

89 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
90 [assignment: list of TSF data]
91 [assignment: the authorised identified roles]
92 [assignment: types of emissions]
93 [assignment: specified limits]
94 [assignment: list of types of TSF data]
95 [assignment: list of types of user data]
96 [assignment: type of users]
97 [assignment: type of connection]
98 [assignment: list of type of TSF data]
99 [assignment: list of type of user data]
100 [assignment: list of types of failures in the TSF]

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

FPT_PHP.3 Resistance to Physical Attack

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[101] to the *TSF*[102] by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up and at the conditions *that critical commands are sent to the TOE*[103] to demonstrate the correct operation of the TSF[104].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF Data[105].

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

6.3 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 EAL 4 augmented with the following component:

- ALC_DVS.2 (Sufficiency of security measures).

101 [assignment: physical tampering scenarios]
102 [assignment: list of TSF devices/elements]
103 [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]]
104 [selection: [assignment: parts of TSF], the TSF]
105 [selection: [assignment: parts of TSF data], TSF data]

6.4 SECURITY REQUIREMENTS DEPENDENCIES

6.4.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

The dependence of security functional requirements for the composite TOE on security functional requirements are defined in the following table.

Table 11: Dependency of Composite TOE SFRs

No	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 — FCS_CKM.4	— FCS_COP.1/ENC, FCS_COP.1/MAC — 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 — FCS_CKM.4	— Not fulfilled but justified. See Explanation 1 — Not fulfilled but justified. See Explanation 1
5.	FCS_COP.1/ENC	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— FCS_CKM.1 — FCS_CKM.4
6.	FCS_COP.1/AUTH	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— Not fulfilled but justified. See Explanation 2 — Not fulfilled but justified. See Explanation 2

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
7.	FCS_COP.1/MAC	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— FCS_CKM.1 — FCS_CKM.4
8.	FCS_RND.1	None	
9.	FCS_COP.1/SIG_MRD	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— Not fulfilled but justified. See Explanation 5 — 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	None	
16.	FIA_AFL.1	— FIA_UAU.1	— FIA_UAU.1
17.	FDP_ACC.1/BAC	— FDP_ACF.1	— FDP_ACF.1/BAC
18.	FDP_ACC.1/BAP	— FDP_ACF.1	— FDP_ACF.1/BAP
19.	FDP_ACF.1/BAC	— FDP_ACC.1 — FMT_MSA.3	— FDP_ACC.1/BAC — Not fulfilled but justified. See Explanation 3
20.	FDP_ACF.1/BAP	— FDP_ACC.1	— FDP_ACC.1/BAP

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
		— FMT_MSA.3	— Not fulfilled but justified. See Explanation 6
21.	FDP_UCT.1	— FTP_ITC.1 or FTP_TRP.1 — FDP_ACC.1 or FDP_IFC.1	— Not fulfilled but justified. See Explanation 4 — FDP_ACC.1/BAC, FDP_ACC.1/BAP
22.	FDP_UIT.1	— FDP_ACC.1 or FDP_IFC.1 — FTP_ITC.1 or FTP_TRP.1	— FDP_ACC.1/BAC, FDP_ACC.1/BAP — Not fulfilled but justified. See Explanation 4
23.	FMT_SMF.1	None	
24.	FMT_SMR.1	— FIA_UID.1	— FIA_UID.1
25.	FMT_LIM.1	— FMT_LIM.2	— FMT_LIM.2
26.	FMT_LIM.2	— FMT_LIM.1	— FMT_LIM.1
27.	FMT_MTD.1/INI_ENA	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1 — FMT_SMF.1
28.	FMT_MTD.1/INI_DIS	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1 — FMT_SMF.1
29.	FMT_MTD.1/KEY_WRITE	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1 — FMT_SMF.1
30.	FMT_MTD.1/KEY_READ	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1 — FMT_SMF.1

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
31.	FPT_EMSEC.1	None	
32.	FPT_FLS.1	None	
33.	FPT_PHP.3	None	
34.	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 no necessity to generate nor to 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/BAC 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 SFRs FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRD and the BIS. There is no need for SFR FTP_ITC.1, e.g., to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

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

Explanation 6: The access control TSF according to FDP_ACF.1/BAP 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.

6.4.2 SECURITY ASSURANCE REQUIREMENTS DEPENDENCIES

The EAL 4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not

require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL 4 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 MRD's development and manufacturing especially for the secure handling of the MRD's material.

The component ALC_DVS.2 augmented to EAL 4 has no dependencies to other security requirements.

6.5 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The coverage of the TOE Security Objectives by the SFRs is given in Table 12. The rationale behind this coverage is also given in this section.

Table 12: 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_MRD									✓
FCS_RND.1	✓	✓	✓						
FIA_UID.1			✓	✓					
FIA_AFL.1			✓	✓					
FIA_UAU.1			✓	✓					
FIA_UAU.4	✓	✓	✓						
FIA_UAU.5	✓	✓	✓						
FIA_UAU.6	✓	✓	✓						

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_API.1									✓
FDP_ACC.1/BAC	✓	✓	✓						
FDP_ACC.1/BAP	✓	✓	✓						
FDP_ACF.1/BAC	✓	✓	✓						
FDP_ACF.1/BAP	✓	✓	✓						
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 MRD" addresses the access control of the writing the logical MRD. The write access to the logical MRD data is defined by the SFRs FDP_ACC.1/BAC and FDP_ACF.1/BAC 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 write access to the logical IDL data, however, is defined by the SFRs FDP_ACC.1/BAP and FDP_ACF.1/BAP as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG14 of the logical IDL only once.

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

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 MRD stored on the MRD's chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFRs FDP_ACC.1/BAC and FDP_ACF.1/BAC 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/BAC, 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/BAC, rule 1). The write access to the logical IDL data, however, is defined by the SFRs FDP_ACC.1/BAP and FDP_ACF.1/BAP in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG14 of the logical IDL (FDP_ACF.1.2/BAP, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG14 of the logical IDL (cf. FDP_ACF.1.4/BAP, rule 1). 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 the SFRs 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 MRD data by means of the BAC/BAP mechanism. The SFRs FIA_UAU.6, FDP_UCT.1, and FDP_UIT.1 require, 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 or the logical IDL data groups EF.DG1 to EF.DG14. 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 FDP_ACC.1/BAC and FDP_ACF.1.2/BAC (the read access to the logical IDL data, however, is defined by FDP_ACC.1/BAP and FDP_ACF.1.2/BAP): the successfully authenticated Personalization Agent is allowed to read the data of the logical MRD. The successfully authenticated Basic Inspection System is allowed to read the data of the logical MRD 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 (or Basic Access Protection Configuration 1 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 (or Basic Access Protection Configuration 1 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 SFRs 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, Basic Access Protection Configuration 1 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 MRD’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 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 MRD'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 MRD'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 SFRs FPT_FLS.1 and FPT_TST.1, and/or by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

OT.Prot_Phys-Tamper:

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

OT.Prot_Malfunction:

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

OT.Prot_Abuse-Func:

The security objective OT.Prot_Abuse-Func "Protection against Abuse of Functionality" is ensured by the SFRs 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, proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/SIG_MRD and FCS_COP.1/SHA. It is performed using an internally stored confidential private key as required by FMT_MTD.1/KEY_WRITE and FMT_MTD.1/KEY_READ.

Protection against SPA, DFA and DPA is addressed by OT.Prot_Inf_Leak.

6.6 SECURITY ASSURANCE REQUIREMENTS RATIONALE

An assurance level of EAL 4 with the augmentation ALC_DVS.2 is required for this type of TOE since it is intended to have the capability 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

7.1 SECURITY FEATURES

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.

7.1.1 SF_PP: PHYSICAL PROTECTION

SF_PP, Physical Protection is mainly inherited from the Security IC part (TSF.Control and TSF.Protection of the platform) of composite product to AKIS GEZGIN. For detailed information about the security features provided by the platform, please see Security IC ST [5]. 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 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.

7.1.2 SF_DPM: DEVICE PHASE MANAGEMENT

Device Phase Management security feature is fulfilled by Security IC part of the composite product and the Embedded Software. The Security Feature inherited from the Security IC Platform is TSF.Service of the platform. For the security features provided by the platform, please see the Security IC ST [5].

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

7.1.3 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, and 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 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 create eMRTD / IDL application,
- to write and to read the data of the EF.COM, EF.SOD, EF.DGs of the logical MRD 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 EF.COM, EF.SOD, and EF.DGs of the logical MRD.

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 allowed to read the data in EF.COM, EF.SOD, standard data in EF.DG1 to EF.DG14 of the logical IDL after successful authentication,
- is not allowed to read the biometric data (e.g., data in EF.DG3 and EF.DG4) of the logical MRTD,
- is not allowed to read the biometric data (e.g., data in EF.DG7 and EF.DG8) of the logical IDL.

No terminal is allowed

- to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
- to modify any of the EF.DG1 to EF.DG14 of the logical IDL,
- to read any of the EF.DG1 to EF.DG16 of the logical MRTD without authentication,
- to read any of the EF.DG1 to EF.DG14 of the logical IDL 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 covered by SF_AC are FDP_ACC.1/BAC, FDP_ACC.1/BAP, FDP_ACF.1/BAC, FDP_ACF.1/BAP, FDP_UCT.1, FDP_UIT.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, and FMT_MTD.1/KEY_READ.

Remaining SFRs covered by SF_AC are FMT_SMF.1 and FMT_SMR.1 which require the management functions and management roles.

7.1.4 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/BAP 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/BAP).

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, and FDP_UIT.1.

7.1.5 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,
- Basic Access Protection Configuration 1 Authentication Mechanism,
- Symmetric Authentication Mechanism based on AES,
- Active Authentication.

The Basic Inspection System authenticates to the TOE by means of Basic Access Control Authentication Mechanism (or Basic Access Protection Configuration 1 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, Basic Access Protection Configuration 1 Authentication Mechanism, and the Symmetric Authentication Mechanism. After successful authentication of the terminal with Basic Access Control Authentication Mechanism (or Basic Access Protection Configuration 1 Authentication Mechanism), the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC/BAP 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 (or Basic Access Protection Configuration 1 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 [11] for eMRTD ([25] for IDL) (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, FCS_COP.1/SIG_MRD, FCS_COP.1/AUTH, and FCS_RND.1 are covered.

7.2 SECURITY FUNCTIONS RATIONALE

Table 13 shows the assignment of security functional requirements to TOE's security functionality.

Table 13: 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_MRD					✓

Security Functional Requirement	SF_PP	SF_DPM	SF_AC	SF_SM	SF_IA
FCS_RND.1					✓
FIA_UID.1					✓
FIA_AFL.1					✓
FIA_UAU.1					✓
FIA_UAU.4					✓
FIA_UAU.5					✓
FIA_UAU.6					✓
FIA_API.1					✓
FDP_ACC.1/BAC			✓		
FDP_ACC.1/BAP			✓		
FDP_ACF.1/BAC			✓		
FDP_ACF.1/BAP			✓		
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 STATEMENT OF COMPATIBILITY

This section includes the statement of compatibility between the current Composite Security Target and the Security Target of the underlying hardware.

8.1 PP CONFORMANCE RATIONALE

Contents of this section was removed in Security Target Lite.

8.2 PLATFORM CONFORMANCE RATIONALE

Contents of this section was removed in Security Target Lite.

8.3 COMPATIBILITY: SECURITY REQUIREMENTS

8.3.1 SECURITY FUNCTIONAL REQUIREMENTS

The security requirements of the composite TOE can be mapped directly to the platform SFRs.

Table 14: Platform SFRs - Compatibility Statement

No	Platform SFR	Category[106]	Related TSF
1.	FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3
2.	FRU_FLT.2	RP_SFR-MECH	FPT_TST.1
3.	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1
4.	FDP_IFC.1	RP_SFR-MECH	FPT_EMSEC.1
5.	FPT_TST.1	RP_SFR-MECH	Covered by ADV_IMP.1
6.	FDP_ITT.1	RP_SFR-MECH	FPT_EMSEC.1

7.	FPT_ITT.1	RP_SFR-MECH	FPT_EMSEC.1
8.	FMT_LIM.1	RP_SFR-MECH	FMT_LIM.1
9.	FMT_LIM.1/Loader	RP_SFR-MECH	Covered by ADV_IMP.1
10.	FMT_LIM.2	RP_SFR-MECH	FMT_LIM.2
11.	FMT_LIM.2/Loader	RP_SFR-MECH	Covered by ADV_IMP.1
12.	FCS_RNG.1/PTG.2	IP_SFR	
13.	FCS_RNG.1/DRG.4	RP_SFR-SERV	FCS_RND.1
14.	FCS_RNG.1/PTG.3	IP_SFR	
15.	FCS_COP.1/TDES	IP_SFR	
16.	FCS_COP.1/TDES_LIB	RP_SFR-SERV	FCS_CKM.1 FCS_COP.1/ENC FCS_COP.1/MAC
17.	FCS_COP.1/AES	IP_SFR	
18.	FCS_COP.1/AES_LIB	RP_SFR-SERV	FCS_COP.1/AUTH
19.	FCS_CKM.4/TDES	IP_SFR	
20.	FCS_CKM.4/TDES_LIB	RP_SFR-MECH	Covered by ADV_IMP.1
21.	FCS_CKM.4/AES	IP_SFR	
22.	FCS_CKM.4/AES_LIB	RP_SFR-MECH	Covered by ADV_IMP.1
23.	FAU_SAS.1	RP_SFR-MECH	FAU_SAS.1
24.	FDP_ACC.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1

25.	FDP_ACF.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
26.	FDP_UCT.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
27.	FDP_UIT.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
28.	FDP_SDC.1	RP_SFR-MECH	FPT_PHP.3
29.	FDP_SDI.2	RP_SFR-MECH	FPT_PHP.3
30.	FTP_ITC.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
31.	FCS_COP.1/RSA	RP_SFR-SERV	FCS_COP.1/SIG_MRD
32.	FCS_CKM.5/RSA_PubKeyDerivation	RP_SFR-SERV	FCS_COP.1/SIG_MRD
33.	FCS_CKM.1/RSA_KeyGen	IP_SFR	
34.	FCS_CKM.4/RSA	RP_SFR-MECH	Covered by ADV_IMP.1
35.	FCS_COP.1/ECDSA	RP_SFR-SERV	FCS_COP.1/SIG_MRD
36.	FCS_COP.1/ECC_DHKE	IP_SFR	
37.	FCS_CKM.1/ECC_KeyGen	IP_SFR	
38.	FCS_CKM.4/ECC	RP_SFR-MECH	Covered by ADV_IMP.1
39.	FCS_COP.1/SHA	RP_SFR-SERV	FCS_CKM.1 FCS_COP.1/SHA FCS_COP.1/SIG_MRD
40.	FMT_SMF.1	RP_SFR-MECH	FPT_FLS.1 FPT_PHP.3

41.	FDP_ACC.1/ACP	RP_SFR-MECH	FPT_FLS.1
42.	FDP_ACF.1/ACP	RP_SFR-MECH	FPT_FLS.1
43.	FMT_MSA.1/ACP	RP_SFR-MECH	FPT_EMSEC.1 FPT_FLS.1 FPT_PHP.3
44.	FMT_MSA.3/ACP	RP_SFR-MECH	FPT_EMSEC.1 FPT_FLS.1 FPT_PHP.3
45.	FCS_COP.1/AES_PUF	IP_SFR	
46.	FCS_COP.1/MAC_PUF	IP_SFR	
47.	FCS_CKM.1/PUF	IP_SFR	
48.	FCS_CKM.4/PUF	IP_SFR	

8.3.2 SECURITY ASSURANCE REQUIREMENTS

The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2.

The chosen level of assurance of the platform is EAL 6 augmented with ALC_FLR.1 and ASE_TSS.2.

This shows that the Assurance Requirements of the TOE matches the Assurance Requirements of the hardware.

9 ABBREVIATIONS AND DEFINITIONS

3DES: Triple DES

AA: Active Authentication

AES: Advanced Encryption Standard

APDU: Application Protocol Data Unit

ARR: Access Rules Reference

BAC: Basic Access Control

BAP: Basic Access Protection

BIS: Basic Inspection System

BIS-PACE: Basic Inspection System with PACE

CA: Chip Authentication

CAN: Card Access Number

CPU: Central Processing Unit

CSCA: Country Signing Certification Authority

CVCA: Country Verifying Certification Authority

DES: Data Encryption Standard

DF: Dedicated File

DFA: Differential Fault Analysis

DPA: Differential Power Analysis

EAC: Extended Access Control

EAL: Evaluation Assurance Level

ECC: Elliptic Curve Cryptography

EF: Elementary File

EIS: Extended Inspection System

ES: Embedded Operating System

GIS: General Inspection System

IC: Integrated Circuit

ICAO: International Civil Aviation Organization

IDL: ISO-compliant Driving License

MF: Master File

MRD: Machine Readable Document

MRTD: Machine Readable Travel Document

MRZ: Machine Readable Zone

N/A: Not Applicable

NVM: Non-Volatile Memory

OSP: Organizational Security Policy

PA: Passive Authentication

PACE: Password Authenticated Connection Establishment

PP: Protection Profile

RAM: Random Access Memory

RSA: Ron Rivest, Adi Shamir and Leonard Adleman

ROM: Read Only Memory

SAC: Supplemental Access Control

SAI: Scanning Area Identifier

SAR: Security Assurance Requirements

SHA: Secure Hash Algorithm

SPA: Simple Power Analysis

SFR: Security Functional Requirement

ST: Security Target

TA: Terminal Authentication

TOE: Target of Evaluation

TPDU: Transmission Protocol Data Unit

10 REFERENCES

[1] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014

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

[3] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 (version 1.3.2, 05th December 2012)

[4] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2nd November 2011, BSI-CC-PP-0068-V2-2011

[5] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, Rev. 2.6, 13 June 2022

[6] Common Criteria for Information Technology Security Evaluation Part I: Introduction and General Model; Version 3.1 Revision 5 CCMB-2017-04-001

[7] Common Criteria for Information Technology Security Evaluation Part II: Security Functional Requirements; Version 3.1 Revision 5 CCMB-2017-04-002

[8] Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 3.1 Revision 5 CCMB-2017-04-003

[9] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, CCMB-2017-04-004

[10] ICAO Doc 9303, Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometric and Other Data in the Contactless Integrated Circuit (IC), Eighth Edition, 2021, International Civil Aviation Organization

[11] ICAO Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, Eighth Edition, 2021, International Civil Aviation Organization

[12] ISO/IEC 14888-3:2018 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, Fourth edition, 2018-11-01

[13] ISO/IEC 9796-2 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms, 2010-12-15

[14] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, 2001, U.S. Department of Commerce, National Institute of Standards and Technology

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

[16] FIPS PUB 180-4, Secure Hash Standard (SHS), Federal Information Processing Standards Publication, August 2015, U.S. Department of Commerce, National Institute of Standards and Technology

[17] FIPS PUB 197 Advanced Encryption Standard (AES), November 26, 2001

[18] ISO 1177 Information processing — Character structure for start/stop and synchronous character oriented transmission, 1985-07-25

[19] ISO 14443-3 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision, Fourth edition, 2018-07

[20] ISO 14443-4 Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol, Fourth edition, 2018-07

[21] ISO 7816-4 Information Technology – Identification Cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, Third edition, 2013-04-15

[22] ISO 7816-8 Information Technology – Identification Cards – Integrated circuit cards – Part 8: Commands and mechanisms for security operations, Third edition, 2016-11-01

[23] ISO 7816-9 Information Technology – Identification Cards – Integrated circuit cards – Part 9: Commands for card management, Third edition, 2017-12-15

[24] ISO 18013-2:2020 Personal identification – ISO-compliant driving licence Part 2: Machine-readable technologies, Second edition, 2020-06

[25] ISO 18013-3:2017+A2:2023 Information technology – Personal identification – ISO-compliant driving licence Part 3: Access control, authentication and integrity validation, Second edition, 2017-04

[26] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI)