TÜBİTAK BİLGEM UEKAE

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

eID Applications Unit

SECURITY TARGET LITE

of

AKIS GEZGIN_N v1.0.1.0

SAC & EAC Configuration

Revision no	02
Revision date	18.01.2021
Document code	AKiS-GEZGiN_N-SAC&EAC-ST_Lite-02
Prepared by	eID Applications Unit
Approved by	AKİS Project Manager

REVISION HISTORY

Revision #	Revision Reason	Date
1.	First public version of the ST created	06.11.2020
2.	Updated due to TOE version 1.0.1.0	18.01.2021

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: Security Target Lite of AKIS GEZGIN_N v1.0.1.0 SAC & EAC Configuration

Document Version: 02

CC Version: 3.1 (Revision 5)

Assurance Level: EAL 5+ (ALC_DVS.2, AVA_VAN.5)

1.2 TOE REFERENCE

The current Security Target refers to the product AKIS GEZGIN_N SAC & EAC Configuration. Version number of the TOE is 1.0.1.0.

1.3 TOE OVERVIEW

The Target of Evaluation (TOE) addressed by this security target is AKIS GEZGIN_N SAC & EAC Configuration. This TOE is the composition of the contactless smartcard chip P71D320P of NXP SmartMX3 platform with embedded software including the electronic Machine Readable Travel Document (eMRTD) application with Extended Access Control (EAC) and Supplemental Access Control (SAC) mechanisms. 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 SAC & EAC Configuration”.

The term Supplemental Access Control (SAC) is based on Password Authenticated Connection Establishment (PACEv2).

The TOE comprises the following:

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

1.3.1 TOE TYPE AND USAGES OF THE TOE

The TOE type is a contactless smart card chip with embedded software including the eMRTD application. The composite product conforms to eMRTD specifications (AA, BAC, SAC and EAC). The TOE is designed and developed to be used as e-Passport (eMRTD). Personalization Agent selects the security features to be configured in the TOE depending on the governmental policies.

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

Table 1: Features supported by the TOE

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

1.3.2 MAJOR SECURITY PROPERTIES OF THE TOE

The following security services are provided within the scope of the TOE:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support.
- Passive Authentication (PA),
- Supplemental Access Control (SAC),
- Extended Access Control (EAC),
- Cryptosystem migration (Algorithm change during certificate verification transaction).

1.3.2.1 PASSIVE AUTHENTICATION (PA)

Passive Authentication (PA) ensures that the contents of the TOE is authentic and tamper-proof and therefore has not changed since personalization. The TOE contains a file (SOD), placed under the corresponding application during personalization. This SOD file, located under the eMRTD application, stores 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.

1.3.2.2 SUPPLEMENTAL ACCESS CONTROL (SAC)

Supplemental Access Control (SAC) is introduced by ICAO as a supplement to Basic Access Control (BAC) to strengthen the security.

SAC is a security mechanism to protect data stored in the TOE. SAC specifies the Password Authenticated Connection Establishment (PACE) protocol which supplements and improves Basic Access Control. Similar to BAC, PACE is developed to prevent two types of attacks: skimming and eavesdropping.

The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password based authentication of the TOE and the TOE environment (inspection system). For TOE configured to support SAC, the supported algorithms are listed in EF.CardAccess file. If no such file exists, the TOE environment may choose to proceed with BAC.

Throughout this document, the term PACE refers to PACE v2. The ICAO Technical Report "Supplemental Access Control" [19] describes how to migrate from the current access control mechanism, Basic Access Control, to PACE v2, a new cryptographically strong access control mechanism that is initially provided supplementary to Basic Access Control.

1.3.2.3 EXTENDED ACCESS CONTROL (EAC)

Extended Access Control (EAC) is typically used to provide confidentiality of the biometric data stored under the application. EAC enhances the security features of the TOE by adding functionality to check the authenticity of both the chip (via chip authentication) and the TOE environment (via terminal authentication). EAC ensures a strong mutual authentication between the TOE and the TOE environment and therefore provides a stronger encryption than BAC.

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the chip. The protocol establishes Secure Messaging between the chip and a terminal using Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) static key pair stored on the chip. Chip Authentication Private Key is stored on the secure memory of the chip whereas public key and the domain parameters are stored in data group

14 (DG14). The personalization agent decides what key(s) to store in DG14 based on governmental policies. The terminal reads DG14 and decides which key to use if multiple options are available; otherwise, the terminal uses the specified key. The terminal reads (EC)DH public key and domain parameters from DG14 on the chip, generates an ephemeral (EC)DH key pair and then sends the ephemeral public key to the chip. Finally, both the chip and the terminal compute the new session key.

Chip Authentication is an alternative to the Active Authentication, i.e., it enables the terminal to verify that the chip is genuine but has two advantages over the original protocol:

- Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the MRTD, this protocol also provides strong session keys.

The protocol provides implicit authentication of both the chip itself and the stored data by performing Secure Messaging using the new session keys (3DES, AES128, AES192, and AES256). After a successful execution of Chip Authentication, strong session encryption is established rendering the decryption of an eavesdropped communication computationally impossible. In addition, the chip restricts access rights to require Secure Messaging established by Chip Authentication.

For Chip Authentication with DH, the respective algorithms and formats from Table 2 shall be used:

Table 2: Object Identifiers for Chip Authentication with DH

OID	Sym. Cipher	Key Length	Secure Messaging	Auth. Token
id-CA-DH-3DES-CBC-CBC	3DES	112	CBC/CBC	CBC
id-CA-DH-AES-CBC-CMAC-128	AES	128	CBC/CMAC	CMAC
id-CA-DH-AES-CBC-CMAC-192	AES	192	CBC/CMAC	CMAC
id-CA-DH-AES-CBC-CMAC-256	AES	256	CBC/CMAC	CMAC

For Chip Authentication with ECDH, the respective algorithms and formats from Table 3 shall be used:

Table 3: Object Identifiers for Chip Authentication with ECDH

OID	Sym. Cipher	Key Length	Secure Messaging	Auth. Token
id-CA-ECDH-3DES-CBC-CBC	3DES	112	CBC/CBC	CBC
id-CA-ECDH-AES-CBC-CMAC-128	AES	128	CBC/CMAC	CMAC
id-CA-ECDH-AES-CBC-CMAC-192	AES	192	CBC/CMAC	CMAC

id-CA-ECDH-AES-CBC-CMAC-256	AES	256	CBC/CMAC	CMAC

For the terminal authentication, the terminal (the TOE environment or the inspection system) sends a Card Verifiable Certificate (CVC) chain to the TOE. Upon verification of the certificate chain, the public component of RSA or ECC key is sent to the TOE. Terminal selects the cryptographic key (either ECC or RSA Key) to be sent among the keys defined in the TOE in EF.CVCA file.

TOE environment signs the data composed of document number, a random number and CA public key information using the private component of this public key and sends the signed data to the TOE which then verifies the signature with the public component. At the end of this process, the TOE environment is authenticated to be able to read biometric data from the TOE.

Throughout this document, the term EAC refers to EAC v1.

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

In order to be powered up and to communicate with the ‘external world’, the TOE needs a terminal (card reader) supporting the contactless communication according to [35] and [36].
When a terminal starts a communication session using SAC, the TOE, from the logical point of view, shall be able to recognize the terminal type “Basic Inspection System with PACE” and it requires the terminal to provide evidence of possessing authorization information (a shared secret) before access according to [19] is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

1.5 TOE DESCRIPTION

1.5.1 PHYSICAL AND LOGICAL SCOPE OF THE TOE

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

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

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

A logical TOE will have data of the TOE holder stored according to the Logical Data Structure as specified by ICAO 9303 [12] on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the TOE holder.

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

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

The TOE comprises the following:

- the circuitry of the eMRTD's chip (contactless smartcard chip P71D320P of NXP SmartMX3 platform),
- the IC Dedicated Software with the parts IC Dedicated Test & Support Software and Symmetric Crypto Library
- the Asymmetric Crypto Library Cobalt,
- the IC Embedded Software including operating system and eMRTD application,
- the associated guidance documentation.

All components of the TOE are listed in Table 4.

Table 4: Components of the TOE

Type	Name	Version	Form of Delivery
IC Hardware	N7021	VA	Wafer, modules and package
IC Dedicated Software	Test & Boot Software	20.0	On-chip software
Symmetric Crypto Library	Crypto Library Iron	2.0.6-01	On-chip software
Asymmetric Crypto Library	Crypto Library Cobalt on N7021	2.08	On-chip software
Security IC Embedded Software and eMRTD application	AKIS GEZGIN_N	1.0.1.0	On-chip software
Document	AKIS GEZGIN_N v1.0.1.0 SAC & EAC Configuration Yönetici ve Kullanıcı Kılavuzu	8	DOC or PDF via hand-delivery

Document	AKIS GEZGIN_N v1.0.1.0 SAC & EAC Configuration Teslim ve İşletim Dokümanı	07	DOCX or PDF via hand-delivery

1.5.1.1 LDS APPLICATION

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

The generic file system is given in the Figure 1.

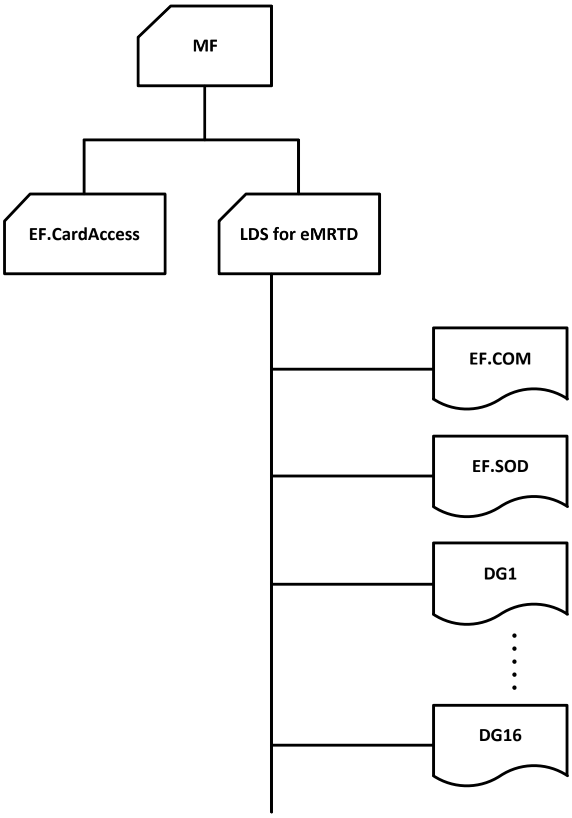


Figure 1: Generic file system of the TOE

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

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

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

1.5.1.1.1 SYSTEM FILES

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

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

In particular, these files are used to store:

- EAC Chip Authentication Private Key,
- EAC Terminal Authentication Public Key.

1.5.1.1.2 DATA FILES

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

Common Data Files are as follows:

- EF.CardAccess which contains the parameters (i.e., symmetric ciphers, key agreement algorithms, domain parameters, and mappings) supported by the TOE and to be used for PACE,
- 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,
- DG1 up to DG16 which contain information about the eMRTD holder (picture, name…) and key required to perform authentications.

1.5.2 INTERFACES

For the electrical I/O:

- ISO 1177 - Information Processing Character Structure For Start/Stop And Synchronous Character Oriented Transmission [34],
- ISO 14443-3 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 3: Initialization and anticollision [35],
- ISO 14443-4 Identification cards — Contactless integrated circuit cards — Proximity cards, Part 4: Transmission protocol [36].

For the commands:

- ISO 7816 Commands [37], [38], [39],
- MRTD Commands [16].

1.5.3 LIFE CYCLE

This Security Target is conformant to the protection profile BSI-CC-PP-0056-V2-2012 and life cycles of the composite product AKIS GEZGIN_N are based on the life cycles of platform ST and given as follows. Note that any TOE-specific details are given in *italics*.

Phase-1: Development

- **(Step1)** The TOE is developed in Phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
- **(Step2)** The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software, the eMRTD application and the guidance documentation associated with these TOE components.
- The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase-2: Manufacturing

- **(Step3)** In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

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

Phase-3: Personalization of the MRTD

- ***(Step6)*** *This phase starts with the successful authentication of personalization key. Another successful authentication is needed to complete this phase. Personal information data are written and access rules are defined in this phase. Application specific restrictions cannot be implemented in personalization phase.*

[1] For the composite product AKIS GEZGIN_N, the IC embedded software hex code is always preloaded onto the flash memory of the chip platform during mass production by the IC manufacturer.

[2] Before activation, the IC embedded software can be removed from IC, for further version upgrades, by the MRTD manufacturer using a cryptogram intended for flash loader activation only.

- The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e., the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.
- The signing of the Document security object by the Document Signer finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase-4: Operational Use

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

Phase-5: Death Phase

- *Death phase is defined by embedded software. TOE becomes out of order and cannot be used as a legitimate one. 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, TOE enters the death phase. In this phase, TOE doesn't accept any commands but the ones that provide limited information about itself.*

1.5.4 TOE CONFIGURATIONS

AKIS GEZGIN_N SAC & EAC Configuration is within the scope of this Security Target. The configuration is done through writing to a special area in the EEPROM area during the Personalization Operation.

1.5.5 PLATFORM INFORMATION

1.5.5.1 PLATFORM IDENTIFICATION

Platform:
NXP Technologies, SmartMX3 P71D320P

Platform ST:
NXP Secure Smart Card Controller N7021 VA Security Target Lite, Rev. 2.3, 2019-06-04
Crypto Library Cobalt on N7021 VA Security Target Lite, Rev. 2.3, 5 June 2019

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+ (ALC_FLR.1)

Platform Certification Report:
BSI-DSZ-CC-0977-V2-2019 for NXP Secure Smart Card Controller N7021 VA including IC Dedicated Software from NXP Semiconductors Germany GmbH
BSI-DSZ-CC-1019-V2-2019 for Crypto Library Cobalt on N7021 VA from NXP Semiconductors Germany GmbH

Common Criteria Version:

- CC v3.1 Revision 5

1.5.5.2 PLATFORM DESCRIPTION

1.5.5.2.1 PRODUCT SPECIFIC FEATURES

- High-performance dual-Interface secure microprocessor
- Top-level cryptography engines with "full key length" support
  - Dedicated cryptography functional unit for symmetric DES and AES algorithms
  - 168-bit (three-key) triple-DES (TDES or 3DES) [3], in various configurations
  - AES with 128, 192 and 256-bit key length
  - Asymmetric cryptography accelerator unit, supporting RSA, ECC and related algorithms
  - RSA cryptography with arbitrary key length up to 4096 bits
  - Elliptic-curve cryptography (ECC) with key length up to 640 bits
- True Random Number Generator, compliant to AIS31

[3] It is stated by the certification authority BSI that although the 2-key version of TDES provides all the security features and satisfies all the security requirements which the 3-key version of TDES does, the 2-key version of TDES is excluded from the scope of hardware platform certification due to mathematical weaknesses.

- Deterministic Random Number Generator for faster execution in cases where lower RNG entropy is sufficient
- Cyclic redundancy check (CRC) functional unit for 16 and 32-bit operation
- Large memory for operating system design flexibility
- NXP FlexMem approach
- Secure bootloader for initial loading or updates of Flash memory; suitable for use in secure manufacturing sites as well as in general environments. Various configuration options exist to manage and delegate rights for access and writing.
- Vertical Firewall technology
    - Full separation of two SW instances (e.g. customer OS and MIFARE emulation), giving equal rights to both of these
    - Security certified sharing / handover mechanism for managing HW resources between SW instances
- Dual-interface support with wide configuration range
- Wide range of packaging options - contact, dual-interface and contactless chip modules, various wafer delivery options
- Hardware-based physically unclonable function (PUF) available for configuration through NXP firmware

Security features

- 90nm CMOS technology offers strong inherent protection against invasive attacks on logic and memories
- NXP Glue Logic concept effectively de-correlates the function and location of circuitry on the device: no functional blocks are recognizable in any physical layer of the device, adding another level of protection against active and passive invasive attacks
- No use of logical hardmacro blocks; all logics in the device - including CPU, coprocessors and all other functions - are synthesized into a single glue logic area.
- NXP PUF (physically unclonable feature) for additional protection of secrets against sophisticated reverse-engineering attacks

Functional diagram

The diagram provides a generic overview of the architecture of the SmartMX3 P71 product family. Functional blocks, pins and connections shown in this diagram are optional and represent a super-set of those elements actually implemented in a real product.

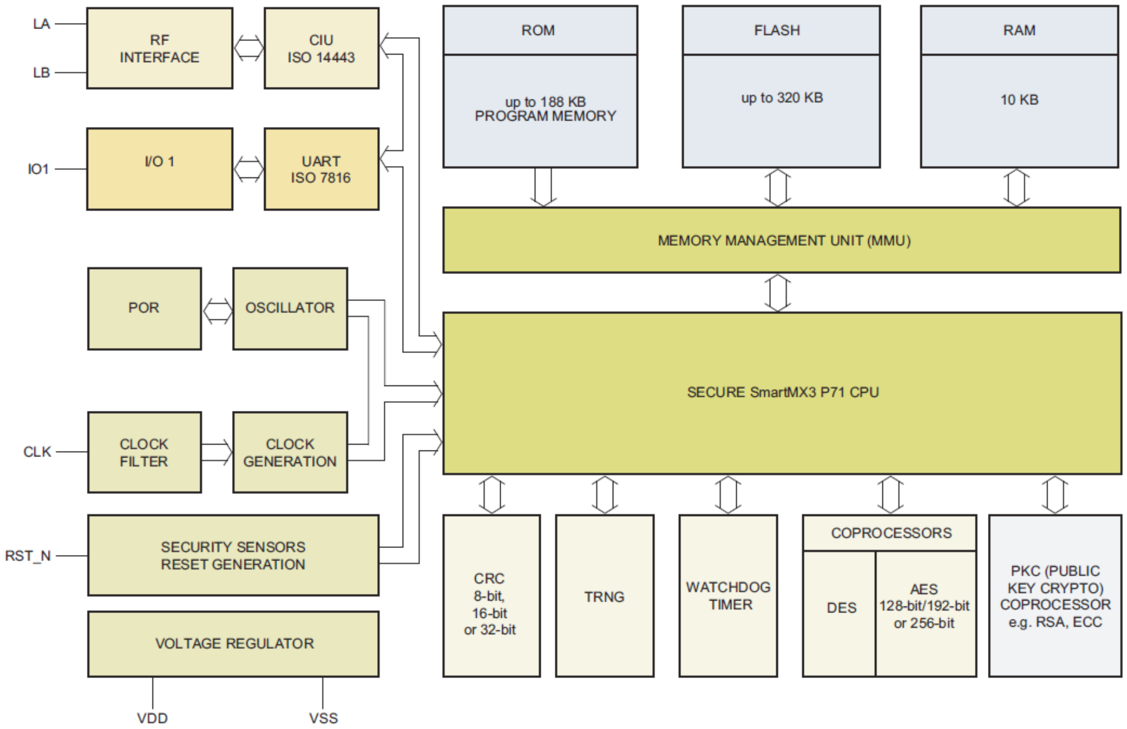


Figure 2 : Functional Diagram of the SmartMX3 P71 product family

1.5.5.2.2 CRYPTO LIBRARY

Symmetric Cipher Library

The Configurable Symmetric Cipher library component supports:

- AES encryption and decryption with key length 128, 192 and 256 bit
- 3-DES encryption and decryption using two single-DES keys
- 3-DES encryption and decryption using three single-DES keys
- ECB mode
- CBC mode
- DF support

RSA Library

The following functions are included within the RSA component (implemented according to [19]):

- RSA public key operation
- RSA private key (in plain format) operation

- RSA private key (in CRT format) operation
- RSA calculation of public exponent from an RSA CRT private key
- RSA calculation of the exact bit length out of a CRT key
- RSA OAEP padding (encode and decode)
- RSA PSS padding (generation and verification)

The supported key length for the public modulus n is between 512 and 4096 bits.

The bit lengths of p and q (for keys in CRT format) is restricted by (bitlength(n)+1)/2+128 bit, i.e. the maximal supported bit difference between p and q is 256 bit.

RSA Key Generation Library

The following functions are included within the RSA component:

- RSA Key Generation (in CRT format)
- Derivation of RSA Key in plain format from RSA Key in CRT format

The supported key length for the public modulus n is between 512 and 4096 bits. The primes p and q are chosen to be congruent to 3 mod 4.

N7021 Crypto Library ECC over GF(p) Library

API functions for the following functionalities are included in the ECC over GF(p) component :

- ECDSA Signature Generation according to ISO/IEC 15946-2 [21], ANSI X9.62 [24] and FIPS 186-4 [23]
- ECDSA Signature Verification according to ISO/IEC 15946-2 [21], ANSI X9.62 [24] and FIPS 186-4 [23]
- EC Key generation according to ISO/IEC 15946-1 [20], ANSI X9.62 [24] and FIPS 186-4 [23]
- EC Point Multiplication according to ISO/IEC 15946-3 [22] and ANSI X9.62 [24]
- EC full point addition according to ISO/IEC 15946-1 [20]
- EC curve parameter verification
- EC pre-computed points calculation as preparation for 1, 2, 3 and 4

The bit lengths for the prime p and the base point order n must not be smaller than 128 bit and must not be greater than 640 bit. Moreover, the co-factor h of supported elliptic curves E is limited to 1. Therefore, the order n of a supported elliptic curve must be prime. In particular, all curves proposed by ANSI X9.62 [24], FIPS 186-4 [23] and the German ECC Brainpool standard are supported.

SHA Library

The SHA library component implements hashing according to the standard [25]. It supports the following algorithms:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

for messages of length equal to an integer number of bytes, up to a maximum length of 2^{61}-1 bytes in length for SHA-1, SHA-224 and SHA-256, and up to a maximum length of 2^{125}-1 bytes in length for SHA-384 and SHA-512.

RNG Library

The RNG library component implements pseudo-random number generation according to the NIST SP 800-90A specification (see ref [26]). The block cipher operations can be selected by the user to run in either DES (3-Key TDEA) or AES (128, 192 or 256) mode.

Hash Library

The Hash library component implements a common interface to the hashing algorithms provided by the hashing components.

2 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 conformance claim is as follows:

- part 2 extended,
- part 3 conformant.

2.1 PP CLAIM

This ST claims strict conformance to 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) [3].

2.2 PACKAGE CLAIM

The current ST is conformant to the following security requirements package: assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in the CC, part 3.

3 SECURITY PROBLEM DEFINITION

The TOE is the composition of the Embedded Software (ES) and the security IC. ES also includes the eMRTD Application.

This section is based on protection profiles BSI-CC-PP-0056-V2-2012 (EAC PP) [3] and BSI-CC-PP-0068-V2-2011 (PACE PP) [4]. For more detailed information, please see EAC PP [3] and PACE PP [4].

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

3.1 ASSETS

3.1.1 ASSETS PROTECTED BY THE EMRTD APPLICATION

Assets protected according to PACE PP are given in Table 5. These assets are protected against advanced attacker.

Table 5: Assets due to PACE PP

Primary Assets			
	Assets	**Definition**	**Protected Against**
1.	User data stored on the TOE	All data (except authentication data) stored in the context of the ePassport application of the travel document and allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. This asset covers User Data on the MRTD's chip, Logical MRTD Data and Sensitive User Data.	Confidentiality Integrity Authenticity
2.	User data transferred between the TOE and the terminal connected (i.e., an authority represented by Basic Inspection	All data (except authentication data) being transferred in the context of the ePassport application of the travel document between the TOE and an authenticated terminal acting as Basic Inspection System	Confidentiality Integrity Authenticity

	System with PACE)	with PACE User data can be received and sent.	
3.	Travel document tracing data	Technical information about the current and previous locations of the travel document (TOE tracing data) gathered unnoticeably (of the travel document holder) by establishing or listening to a communication via the contactless interface of the TOE without in-advance knowledge of any PACE password. TOE tracing data can be provided / gathered.	Unavailability
		Secondary Assets	
	Assets	**Definition**	**Protected Against**
4.	Accessibility to the TOE functions and data only for authorized subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.	Availability
5.	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers Authenticity of the MRTD's chip.	Availability
6.	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7.	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8.	Travel document communication	Restricted-revealable authorization information for a human user being used	Confidentiality Integrity

	establishment authorization data	for verification of the authorization attempts as authorized user (PACE password). These data are stored in the TOE and are not to be sent to it.	

Application Note 1: Please note that user data being referred to in the table above include, amongst others, individual-related (personal) data of the travel document holder which also includes the traveler’s sensitive (i.e., biometric) data.

Application Note 2: Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

Application Note 3: Travel document communication establishment authorization data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorization attempt. The TOE shall secure the reference information as well as – together with the terminal connected – the verification information in the ‘TOE ↔ terminal’ channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be sent to the TOE.

Assets protected according to EAC PP are given in Table 6. These assets are protected against advanced attacker.

Table 6: Assets due to EAC PP

	Assets	Definition	Protected Against
1.	Logical travel document sensitive User Data	Sensitive biometric reference data stored in data groups EF.DG3 and EF.DG4	Confidentiality Integrity Authenticity
2.	Authenticity of the travel document’s chip	The authenticity of the travel document’s chip personalized by the issuing State or Organization for the travel document holder is used by the traveler to prove his or her possession of a genuine travel document.	Availability

3.2 SUBJECTS AND EXTERNAL ENTITIES

This Security Target considers the subjects given in Table 7.

Table 7: Subjects and External Entities of the TOE

Subject	Definition
Travel document holder	The rightful holder of the travel document for whom the issuing State or Organization personalized the travel document.
Traveler	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
Terminal	A terminal is any technical system communicating with the TOE through the contactless interface.

Inspection system (IS)	A technical system used by the border control officer of the receiving State or Organization (i) examining the travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder. The **Basic Inspection System (BIS)** (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the BAC Mechanism and (iii) gets the authorization to read the logical MRTD under the BAC by optical reading the MRTD or other parts of the MRTD book/card providing this information. The **Basic Inspection System with PACE (BIS-PACE)** is a technical system being used by an inspecting authority and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data -face- of the travel document presenter with the stored biometric data -EF.DG2- of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. The **Extended Inspection System (EIS)** performs the Advanced Inspection Procedure and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC, (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information, (iv) implements the Terminal Authentication and Chip Authentication protocols both version 1 according to [5] and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS}). This role is usually delegated to a Personalization Agent.

Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means.
Personalization Agent	The agent is acting on behalf of the issuing State or Organization to personalize the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [12], (iv) writing the document details data, (v) writing the initial TSF data and (vi) signing the Document Security Object defined in [12]. Please note that the role 'Personalization Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Country Verifying Certification Authority	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier	The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
Attacker[4]	A threat agent trying (i) to undermine the security policies, especially to change properties of the assets having to be maintained, (ii) to manipulate the logical travel document without authorization, (iii) to read sensitive biometric reference data (i.e., EF.DG3 and EF.DG4), (iv) to forge a genuine travel document, or (v) to trace a travel document. The attacker is assumed to possess an at most *high* attack potential.

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

3.3 THREATS

Threats of the Composite TOE due to hardware, terminal, communication and application related threats are given in Table 8.

Table 8: Application related threats

#	Threat	Definition
1.	T.Read_Sensitive_Data: Read the sensitive biometric reference data (EAC)	**Adverse action:** An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document’s chip. Note, that the sensitive biometric reference data are stored only on the travel document’s chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well. **Threat agent:** having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document. **Asset:** confidentiality of logical travel document sensitive user data (i.e., biometric reference data)
2.	T.Counterfeit: Counterfeit of travel document chip data	**Adverse action:** An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document’s chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document’s chip used for authentication of a traveler by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document’s chip and copy them on another appropriate chip to imitate this genuine travel document’s chip. **Threat agent:** having high attack potential, being in possession of one or more legitimate travel documents **Asset:** authenticity of user data stored on the TOE

#	Threat	Definition
3.	T.Skimming: Skimming travel document / Capturing Card-Terminal Communication	**Adverse action:** An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE. **Threat agent:** having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. **Asset:** confidentiality of logical eMRTD **Application Note 4:** A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST. **Application Note 5:** MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither of the CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder
4.	T.Eavesdropping: Eavesdropping on the communication between the TOE and the PACE terminal	**Adverse action:** An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected. **Threat agent:** having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. **Asset:** confidentiality of logical travel document data **Application Note 6:** A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST

#	Threat	Definition
5.	T.Tracing: Tracing travel document	**Adverse action:** An attacker tries to gather TOE tracing data (i.e., to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE. **Threat agent:** having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. **Asset:** privacy of the travel document holder **Application Note 7:** This Threat completely covers and extends "T.Chip-ID" from BAC PP [2]. **Application Note 8:** A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST. **Application Note 9:** Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.
6.	T.Forgery: Forgery of data	**Adverse action:** An attacker fraudulently alters the User Data or/and TSF-data stored on the eMRTD or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one. **Threat agent:** having high attack potential **Asset:** integrity of the travel document

#	Threat	Definition
7.	T.Abuse-Func: Abuse of Functionality	**Adverse action:** An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the travel document holder. **Threat agent:** having high attack potential, being in possession of one or more legitimate travel documents. **Asset:** integrity and authenticity of the travel document, availability of the functionality of the travel document. **Application Note 10:** Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here

#	Threat	Definition
8.	T.Information_Leakage: Information Leakage from travel document	**Adverse action:** An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. 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 high attack potential **Asset:** confidentiality of User Data and TSF-data of the travel document

#	Threat	Definition
9.	T.Phys-Tamper: Physical Tampering	**Adverse action:** An attacker may perform physical probing of the travel document in order (i) to disclose TSF-data, or (ii) to disclose/reconstruct the travel document's chip Embedded Software. An attacker may physically modify the travel document in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or TSF-data stored on the travel document. **Threat agent:** having high attack potential, being in possession of one or more legitimate travel documents **Asset:** integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of user data and TSF-data of the travel document **Application Note 11:** Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g., the biometric reference data for the inspection system) or the TSF data (e.g., authentication key of the MRTD) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g., to enable information leakage through power analysis). Physical tampering requires a direct interaction with the TOE internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the 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	Definition
10.	T.Malfunction: Malfunction due to Environmental Stress	**Adverse action:** An attacker may cause a malfunction of the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved, e.g., by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administration functions. To exploit these vulnerabilities an attacker needs information about the functional operation. **Threat agent:** having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation **Asset:** integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of user data and TSF-data of the travel document **Application Note 12:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

3.4 ORGANISATIONAL SECURITY POLICIES

Organizational security policies of the composite TOE is given in Table 9.

Table 9: Composite TOE Policies

#	Policy Name	Definition
1.	P.Manufact: Manufacturing of the travel document's chip	The Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the keys for the authentication of the travel document Manufacturer. The travel document Manufacturer writes the Pre-Personalization Data which contains at least the Personalization Agent key, the Chip Authentication public. The eMRTD Manufacturer is an agent authorized by the Issuing State or Organization only.
2.	P.Pre-Operational: Pre-operational handling of the travel document	1. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations. 2. The eMRTD Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE. 3. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e., before they are in the operational phase. 4. If the travel document issuer authorises a Personalization Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the eMRTD Issuer's policy.

#	Policy Name	Definition
3.	P.Card_PKI: PKI for Passive Authentication (issuing branch)	**Application Note 13:** The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed/made available to their final destination, e.g., by using directory services. 1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e., for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The eMRTD Issuer shall publish the CSCA Certificate (C_{CSCA}). 2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [12], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [12], 5.5.1. 3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.
4.	P.Trustworthy_PKI: Trustworthiness of PKI	The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

#	Policy Name	Definition
5.	P.Terminal: Abilities and trustworthiness of terminals	The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows: 1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [12]. 2. They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie- Hellman). The related terminals need not to use any own credentials. 3. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document). 4. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g., confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.
6.	P.Sensitive_Data: Privacy of sensitive biometric reference data	The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document’s chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

#	Policy Name	Definition
7.	P.Personalization: Personalization of the travel document by issuing State or Organization only	The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

3.5 ASSUMPTIONS

Assumptions for the operational environment of the composite TOE is given in Table 10.

Table 10: Composite TOE Assumptions

#	Assumption Name	Definition
1.	A.Passive_Auth: PKI for Passive Authentication	The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication, i.e., digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer: i. generates the Document Signer Key Pair, ii. hands over the Document Signer Public Key to the CA for certification, iii. keeps the Document Signer Private Key secret and iv. uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and Organizations. It is assumed that the Document Security Object contains only the hash values of the genuine user data.

#	Assumption Name	Definition
2.	A.Insp_Sys: Inspection Systems for global interoperability	The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE and/or BAC. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical eMRTD under PACE or BAC and performs the Chip Authentication v.1 to verify the MRTD and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Justification: The assumption A.Insp_Sys does not confine the security objectives of the [4] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.
3.	A.Auth_PKI: PKI for Inspection Systems	The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control / Extended Access Protocol. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations sign the certificates of the Document Verifier and the Document Verifiers sign the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip. Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication

#	Assumption Name	Definition
		Protocol Version 1.

4 SECURITY OBJECTIVES

This section 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.

This section is based on protection profiles BSI-CC-PP-0056-V2-2012 (EAC PP) [3] and BSI-CC-PP-0068-V2-2011 (PACE PP) [4]. For detailed information, please see EAC PP [3] and PACE PP [4].

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.Data_Integrity: Integrity of Data

The TOE shall ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying). The TOE shall ensure integrity of the User Data and the TSF data during their exchange between the TOE and the authenticated BIS-PACE inspection system.

OT.Data_Authenticity: Authenticity of Data

The TOE shall ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side. The TOE shall ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the BIS-PACE inspection system. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

OT.Data_Confidentiality: Confidentiality of Data

The TOE shall ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE shall ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the authenticated BIS-PACE inspection system.

OT.Tracing: Tracing travel document

The TOE shall prevent gathering TOE tracing data by means of unambiguous identifying the eMRTD remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

OT.Prot_Abuse-Func: Protection against Abuse of Functionality

The TOE shall prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak: Protection against Information Leakage

The TOE shall provide protection against disclosure of confidential User Data and/or TSF-data stored and/or processed by the travel document

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

Application Note 14: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-Tamper: Protection against Physical Tampering

The TOE shall provide protection of the confidentiality and integrity of the User Data, the TSF-data, and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's 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 functionality.

OT.Prot_Malfunction: Protection against Malfunctions

The TOE shall ensure its correct operation. The TOE shall prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is

to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any
contacts), clock frequency or temperature.

OT.Sens_Data_Conf: Confidentiality of sensitive biometric reference data

The TOE shall ensure the confidentiality of the sensitive biometric reference data and other sensitive data related with specific roles by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE shall ensure the confidentiality of the logical eMRTD data during their transmission to the Extended Inspection System. The confidentiality of the sensitive data shall be protected against attacks with high attack potential.

OT.Chip_Auth_Proof: Proof of MRTD’s chip authenticity

The TOE shall support the Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication. The authenticity proof provided by MRTD’s chip shall be protected against attacks with high attack potential.

Application Note 15: The OT.Chip_Auth_Proof implies the travel document’s chip to have (i) a unique identity as given by the travel document’s Document Number, (ii) a secret to prove its identity by knowledge, i.e., a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document’s chip, i.e., a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document’s chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [12] and (ii) the hash value of EF.DG14 in the Document Security Object signed by the Document Signer.

The following TOE security objectives address the aspects of identified threats to be countered *involving TOE’s environment*.

OT.Identification: Identification of the TOE

The TOE shall provide means to store Initialization and Pre-Personalization Data in its non-volatile memory. The Initialization Data provides a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the eMRTD. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

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 in its non-volatile memory for which all the security requirements of the platform are fulfilled.

OT.AC_Pers: Access Control for Personalization of logical MRTD

The TOE shall ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document security object according to LDS and the TSF data can be written by authorized Personalization Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.

Application Note 16: The OT.AC_Pers implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization.

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

4.2.1 ISSUING STATE OR ORGANIZATION

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

OE.Legislative_Compliance: Issuing of the travel document

The eMRTD Issuer shall issue the eMRTD and approve it using the terminals complying with all applicable laws and regulations.

OE.Passive_Auth_Sign: Authentication of travel document by Signature

The CSCA acting on behalf and according to the policy of the travel document Issuer shall (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 (C_{CSCA}) to receiving States and Organizations maintaining its authenticity and integrity.

A Document Signer acting in accordance with the CSCA policy shall (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [12]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [12]. The CSCA shall issue its certificates exclusively to the rightful organisations (DS) and DSs shall sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalization: Personalization of travel document

The issuing State or Organization shall ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the document holder and create biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport/Card (optical personalization) and store them in the travel document (electronic personalization) for the eMRTD holder as defined in [12], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in ICAO 9303 [12] (in the role of a DS).

OE.Auth_Key_Travel_Document: Travel Document Authentication Key

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data: Authorization for Use of Sensitive Biometric Reference Data

The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to highly sensitive reference data of travel document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

4.2.2 DOCUMENT HOLDER

OE.Travel_Document_Holder: Travel document holder Obligations

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

4.2.3 RECEIVING STATE OR ORGANIZATION

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

OE.Terminal: Terminal operating

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems) are used by terminal operators and by travel document holders as defined in [12].
2. The related terminals implement the terminal parts of the PACE protocol [19] of the Passive Authentication [12] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellman).
3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [12]).
5. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g., confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Application Note 17: OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [2].

OE.Exam_Travel_Document: Examination of the physical part of the travel document

The inspection system of the receiving State or Organization shall examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [19] and/or the Basic Access Control [12]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

OE.Prot_Logical_Travel_Document: Protection of data from the logical travel document

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication protocol version 1.

OE.Ext_Insp_Systems: Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

4.3 SECURITY OBJECTIVES RATIONALE

Table 11: Security Objective Rationale due to EAC PP

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prof_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalization	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Read_Sensitive_Data	X													X			X					
T.Counterfeit		X											X		X							
T.Skimming				X	X	X															X	
T.Eavesdropping						X																
T.Tracing							X														X	
T.Abuse-Func								X														
T.Information_Leakage									X													
T.Phys-Tamper											X											
T.Malfunction												X										
T.Forgery			X	X	X			X			X				X			X	X	X		

P.Sensitive_Data	X												X			X					
P.Personalization			X							X							X				
P.Manufact										X											
P.Pre-Operational			X							X							X				X
P.Terminal														X					X		
P.Card_PKI																		X			
P.Trustworthy_PKI																		X			
A.Insp_Sys														X	X						
A.Auth_PKI													X			X					
A.Passive_Auth														X				X			

Table 12: Security Objective Rationale due to PACE PP

	OT.Identification	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Personalization	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance
T.Skimming			X	X	X									X	

T.Eavesdropping					X										
T.Tracing						X								X	
T.Forgery		X	X	X			X		X		X	X	X		
T.Abuse-Func							X								
T.Information_Leakage								X							
T.Phys-Tamper									X						
T.Malfunction										X					
P.Manufact	X														
P.Pre-Operational	X	X									X				X
P.Terminal													X		
P.Card_PKI												X			
P.Trustworthy_PKI												X			
A.Passive_Auth												X			

Table 13: Coverage of Assumptions, Threats or OSPs with Security Objectives and the Rationales

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
T.Read_Sensitive_Data: Read the sensitive biometric	OT.Sens_Data_Conf OE.Authoriz_Sens_Data	The threat **T .Read_Sensitive_Data** "Read the highly sensitive reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of data" requiring that read access to DGs protected by EAC as specified in EF.COM (containing the highly sensitive reference data) is only granted to authorized inspection systems. Furthermore it is required

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
reference data (EAC)	OE.Ext_Insp_Systems	that the transmission of these data ensures the data confidentiality. The authorization bases on Document Verifier certificates issued by the issuing organisation as required by **OE.Authoriz_Sens_Data** "Authorization for use of highly sensitive reference data". The Document Verifier of the receiving organisation has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the highly sensitive reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems
T.Forgery: Forgery of data	OT.AC_Pers, OE.Personalization, OT.Data_Integrity, OT.Data_Authenticity, OT.Prot_Phys-Tamper, OT.Prot_Abuse-Func, OE.Terminal, OE.Passive_Auth_Sign, OE.Exam_Travel_Document	The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective **OT.AC_Pers** requires the TOE to limit the write access for the eMRTD to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives **OT.Data_Integrity** and **OT.Data_Authenticity**, respectively. The objectives **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to **OE.Terminal** and performing the Passive Authentication using the Document Security Object as aimed by **OE.Passive_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally, the examination of the presented MRTD book/card according to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the eMRTD.
T.Counterfeit: Counterfeit of MRTD’s chip	OT.Chip_Auth_Proof, OE.Auth_Key_Travel_Docume	The threat **T.Counterfeit** “Counterfeit of MRTD’s chip data” addresses the attack of unauthorized copy or reproduction of the genuine MRTD’s chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of MRTD’s chip authentication” using an authentication key pair to be generated by the

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
(EAC)	nt, OE.Exam_Travel_Document	issuing State or Organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** "Travel Document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection System has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the MRTD's chip.
T.Abuse-Func: Abuse of Functionality	OT.Prot_Abuse-Func	The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the softcoded security functionality. The security objective **OT.Prot_Abuse-Func** ensures that the usage of functions having not to be used in the operational phase is effectively prevented.
T.Information_Leakage Information Leakage from travel document	OT.Prot_Inf_Leak	The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction, respectively.
T.Phys-Tamper: Physical Tampering (EAC/SAC)	OT.Prot_Phys-Tamper	

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
T.Malfunction: Malfunction due to Environmental Stress	OT.Prot_Malfunction	
T.Skimming: Skimming/Capturing Card-Terminal Communication	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.Travel_Document_Holder	The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless interface. This threat is countered by the security objectives **OT.Data_Integrity**, **OT.Data_Authenticity** and **OT.Data_Confidentiality** through the PACE authentication. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the eMRTD holder himself/herself or by an authorized person or device, and, hence, cannot be captured by an attacker.
T.Eavesdropping: Eavesdropping on the communication between the TOE and the PACE terminal	OT.Data_Confidentiality	The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective **OT.Data_Confidentiality** through a trusted channel based on the PACE authentication.
T.Tracing Tracing MRTD	OT.Tracing, OE.Travel_Document-Holder	The threat **T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives **OT.Tracing** (no gathering TOE tracing data) and **OE.Travel_Document-Holder** (the attacker does not a priori know the correct values of the shared passwords).

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
P.Manufact: Manufacturing of the MRTD's chip	OT.Identification	The OSP **P.Manufact** "Manufacturing of the travel document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.
P.Pre-Operational: Pre-operational handling of the travel document	OT.Identification, OT.AC_Pers, OE.Personalization, OE.Legislative_Compliance	The OSP **P.Pre-Operational** is enforced by the following security objectives: **OT.Identification** is affine to the OSP's property 'traceability before the operational phase'; **OT.AC_Pers** and **OE.Personalization** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorization of Personalization Agents'; **OE.Legislative_Compliance** is affine to the OSP's property 'compliance with laws and regulations.
P.Card_PKI: PKI for Passive Authentication (issuing branch)	OE.Passive_Auth_Sign	The OSP **P.Card_PKI** is enforced by establishing the issuing PKI branch as aimed by the objectives **OE.Passive_Auth_Sign** (for the Document Security Object).
P.Trustworthy_PKI: Trustworthiness of PKI	OE.Passive_Auth_Sign	The OSP **P.Trustworthy_PKI** is enforced by **OE.Passive_Auth_Sign** (for CSCA, issuing PKI branch).
P.Terminal: Abilities and trustworthiness of terminals	OE.Terminal, OE.Exam_Travel_Document	The OSP **P.Terminal** is obviously enforced by the objective OE.Terminal, whereby the one-to-one mapping between the related properties is applicable. Additionally, this OSP is countered by the security objective **OE.Exam_Travel_Document,** that enforces the terminals to perform the terminal part of the PACE protocol.

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
P.Sensitive_Data: Privacy of sensitive biometric reference data	OT.Sens_Data_Conf, OE.Authoriz_Sens_Data , OE.Ext_Insp_Systems	The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DGs containing the sensitive biometric reference data is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems"
P.Personalization: Personalization of the MRTD by issuing State or Organization only	OE.Personalization, OT.AC_Pers, OT.Identification	The OSP **P.Personalization** "Personalization of the travel document by issuing State or Organisation only" addresses (i) the enrolment of the logical eMRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of travel document", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD". Note the IC Manufacturer equips the TOE with the eMRTD manufacturer Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The eMRTD Manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE".
A.Passive_Auth: PKI for Passive Authentication	OE.Passive_Auth_Sign, OE.Exam_Travel_Document	The assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly addressed by **OE.Passive_Auth_Sign** requiring the eMRTD issuer to establish a PKI for Passive Authentication, generating Document Signing private keys only for rightful organisations and requiring the Document Signer to sign exclusively correct Document Security Objects to be stored on a travel document. The security objective for the TOE environment

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
		OE.Passive_Auth_Sign covers the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_Travel_Document** “Examination of the physical part of the travel document”.
A.Insp_Sys: Inspection Systems for global interoperability	OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document	The examination of the MRTD 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_Travel_Document** "Examination of the physical part of the travel document". The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** "Protection of data from the logical MRTD " will require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.
A.Auth_PKI: PKI for Inspection Systems	OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems	The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of highly sensitive reference data" requires the True Root Certificate to limit the read access to highly sensitives by issuing Document Verifier certificates for authorized receiving organisations or Organizations only. The Document Verifier of the receiving organisation is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing organisation has to establish the necessary public key infrastructure.

5 EXTENDED COMPONENTS

This security target uses components defined as extensions to CC part 2. The extended components defined and described for the TOE are:

- Family FAU_SAS (Audit Data Storage)
- Family FCS_RND (Generation of Random Numbers)
- Family FMT_LIM (Limited capabilities and availability)
- Family FPT_EMS (TOE Emanation)
- Family FIA_API (Application Proof of Identity)

See EAC PP [3] for detailed information about the family FIA_API and PACE PP [4] for detailed information about the rest.

5.1 DEFINITION OF THE FAMILY FAU_SAS (AUDIT DATA STORAGE)

FAU_SAS family of the Class FAU (Security Audit) is defined in PACE PP [4] 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 Audit data storage
1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

5.1.1 FAU_SAS.1 AUDIT STORAGE

Hierarchical to: No other components.

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

Dependencies: No dependencies.

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

FCS_RND of the Class FCS (cryptographic support) is defined in PACE PP [4]. 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 the component 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: Generation of random numbers 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 FMT_LIM (Limited Capabilities And Availability)

FMT_LIM of the Class FMT (Security Management) is defined as given in the EAC PP and PACE PP documents [3] and [4]. 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 Limited capabilities and availability
1
2

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.

5.3.1 FMT_LIM.1 LIMITED CAPABILITIES

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.2 Limited availability.

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

5.3.2 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*].

5.4 DEFINITION OF THE FAMILY FPT_EMS

FPT_EMS (TOE emanation) of the Class FPT (Protection of the TSF) is defined as given in PP Documents [3] and [4].

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component Leveling

FPT_EMS TOE emanation
1

FPT_EMS.1 TOE Emanation has two constituents:

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

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

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

5.4.1 FPT_EMS.1 TOE EMANATION

Hierarchical to: No other components

Dependencies: No dependencies

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

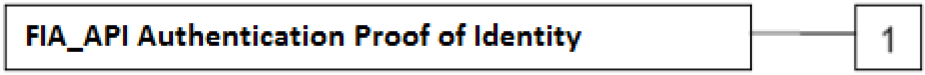
5.5 DEFINITION OF THE FAMILY FIA_API (AUTHENTICATION PROOF OF IDENTITY)

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the EAC PP [3]. 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 Authentication Proof of Identity

Management: FIA_API.1

The following actions could be considered for the management functions in FMT:

Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

5.5.1 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].

6 SECURITY REQUIREMENTS

6.1 OVERVIEW

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part 1 [7]. Each of these operations is used in this ST.

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

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

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

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

Those parts of the sentences originally marked as assignments on SFRs that are defined in CC part 2 but marked as selections on the corresponding SFRs in protection profiles EAC PP [3] and PACE PP [4] are marked as selections in this security target as well.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

This ST is strictly conformant to the protection profiles EAC PP [3] and PACE PP [4]; as a result, all the SFRs in these PP's are included in this security target as well. For details not specifically included in this security target, please see EAC PP [3] and PACE PP [4].

TOE security functional requirements of the composite product are listed in Table 14 and given in Section 6.2.

Table 14: List of SFR's

SFR	Explanation
FCS_CKM.1/DH_PACE	Cryptographic Key Generation - Diffie-Hellman for PACE session keys
FCS_CKM.1/CA	Cryptographic Key Generation - Diffie-Hellman for Chip Authentication session keys

FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/PACE_ENC	Cryptographic Operation - Encryption/Decryption AES/3DES for PACE protocol
FCS_COP.1/PACE_MAC	Cryptographic Operation - MAC for PACE protocol
FCS_COP.1/CA_ENC	Cryptographic Operation - Symmetric Encryption/Decryption for CA protocol
FCS_COP.1/SIG_VER	Cryptographic Operation - Signature verification by travel document
FCS_COP.1/CA_MAC	Cryptographic Operation - MAC for CA protocol
FCS_RND.1	Random number generation
FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorization data
FIA_UID.1/PACE	Timing of identification
FIA_UAU.1/PACE	Timing of authentication
FIA_UAU.4/PACE	Single Use Authentication Mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5/PACE	Multiple Authentication Mechanisms
FIA_UAU.6/PACE	Re-Authenticating - Re-authenticating of Terminal by the TOE
FIA_UAU.6/EAC	Re-Authenticating - Re-authenticating of Terminal by the TOE
FIA_API.1	Authentication Proof of Identity by Chip Authentication
FDP_ACC.1/TRM	Subset access control
FDP_ACF.1/TRM	Security attributes based access control
FDP_RIP.1	Subset residual information protection
FDP_UCT.1/TRM	Basic Data Exchange Confidentiality - MRTD
FDP_UIT.1/TRM	Data Exchange Integrity
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE
FAU_SAS.1	Audit storage
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1/PACE	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_READ	Management of TSF data – Key Read
FMT_MTD.1/PA	Management of TSF data – Personalization Agent
FMT_MTD.1/CVCA_INI	Management of TSF data – Initialization of CVCA Certificate and Current Date
FMT_MTD.1/CVCA_UPD	Management of TSF data – Country Verifying Certification Authority
FMT_MTD.1/DATE	Management of TSF data – Current date
FMT_MTD.1/CAPK	Management of TSF data – Chip Authentication Private Key
FMT_MTD.1/KEY_CHANG	Management of TSF data – Key Change
FMT_MTD.3	Secure TSF data
FPT_EMS.1	TOE Emanation
FPT_FLS.1	Failure with Preservation of Secure State
FPT_TST.1	TSF Testing
FPT_PHP.3	Resistance to Physical Attack

6.2.1 CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_CKM.1/DH_PACE Cryptographic Key Generation - Diffie-Hellman for PACE session keys

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm based on (i) Diffie-Hellman key derivation Protocol compliant to PKCS#3 and (ii) ECDH compliant to [20]

[5] and specified cryptographic key sizes *bit length of the modulus equal to 1024 or 2048 and bit length of the exponent equal to or shorter than 2048 for (i) and 192, 224, 256, 320, 384, 512 bits for (ii)*[6] that meet the following: *[19]*[7].

Application Note 18: The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [19]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e., modulo arithmetic based cryptographic algorithm) or on the ECDH compliant to TR-03111 (i.e., the elliptic curve cryptographic algorithm ECKA). The shared secret value *K* is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}) for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application Note 19: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [19].

Application Note 20: Following the BSI recommendations stated on the certification report of Crypto Library Cobalt on N7021 VA, RSA key lengths below 1976 bits and EC key lengths below 250 bits are out of context for the certification.

FCS_CKM.1/CA Cryptographic Key Generation - Diffie-Hellman for Chip Authentication session keys

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on the (i) Diffie-Hellman key derivation Protocol compliant to PKCS#3 and (ii) ECDH compliant to [20]* [8] and specified cryptographic key sizes of *bit length for modulus up to 2048 for (i) and 128 bits - 640 bits for (ii)* [9] that meet the following: [25] and [17] for (i) and [20] for (ii) [10].

Application Note 21: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [17].

Application Note 22: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1. This protocol may be based on the Diffie-Hellman-Protocol

[5] [“assignment: cryptographic key generation algorithm” in CC part 2; converted to “selection” in PACE PP]
[6] [assignment: cryptographic key sizes]
[7] [assignment: list of standards]
[8] [assignment: cryptographic key generation algorithm]
[9] [assignment: cryptographic key sizes]
[10] [“assignment: list of standards” in CC part 2; converted to “selection” in EAC PP]

compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm) or on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging.

Application Note 23: Due to BSI regulations, the certification of the platform covers standard NIST and Brainpool elliptic curves. As a consequence, the certification of the TOE covers only these elliptic curves as well.

FCS_CKM.4 Cryptographic Key Destruction

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

Application Note 24:

- The TOE shall destroy any session keys in accordance with FCS_CKM.4 after detection of an error in a received command by verification of the MAC and after successful run of the Chip Authentication Protocol v.1.
- The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys.
- The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

FCS_COP.1/PACE_ENC Cryptographic Operation - Encryption/Decryption AES/3DES for PACE protocol

FCS_COP.1.1/PACE_ENC The TSF shall perform *secure messaging - encryption and decryption*[13] in accordance with a specified cryptographic algorithm AES and Triple DES in CBC Mode[14] and cryptographic key sizes 112 bits for 3DES and 128,192, 256 bits for AES[15] that meet the following: *[19]*[16]

[11] [assignment: cryptographic key destruction method]
[12] [assignment: list of standards]
[13] [assignment: list of cryptographic operations]
[14] [“assignment: cryptographic algorithm” in CC part 2; converted to “selection” in PACE PP]
[15] [“assignment: cryptographic key sizes” in CC part 2; converted to “selection” in PACE PP]

Application Note 25: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of the transmitted data and encryption of nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc).

FCS_COP.1/PACE_MAC Cryptographic Operation - MAC for PACE protocol

FCS_COP.1.1/PACE_MAC The TSF shall perform *secure messaging - message authentication code*[17] in accordance with a specified cryptographic algorithm CMAC and Retail MAC[18] and cryptographic key sizes 112 bits for Retail MAC and 128, 192 and 256 bits for CMAC[19] that meet the following: *compliant to [19]*[20].

Application Note 26: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}).

FCS_COP.1/CA_ENC Cryptographic Operation - Symmetric Encryption/Decryption for CA protocol

FCS_COP.1.1/CA_ENC The TSF shall perform *secure messaging - encryption and decryption*[21] in accordance with a specified cryptographic algorithm *AES and 3DES*[22] and cryptographic key sizes *112 bits for 3DES and 128, 192 and 256 bits for AES* [23] that meet the following: *TR-03110, Annex E [16]*[24]

Application Note 27: This SFR requires the TOE to implement the cryptographic primitives (i.e., 3DES and AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

Application Note 28: For the EAC Chip Authentication protocol version 1, the symmetric encryption algorithm to be used for secure messaging is selected by the EIS.

[16] [assignment: list of standards]
[17] [assignment: list of cryptographic operations]
[18] [“assignment: cryptographic algorithm” in CC part 2; converted to “selection” in PACE PP]
[19] [“assignment: cryptographic key sizes” in CC part 2; converted to “selection” in PACE PP]
[20] [assignment: list of standards]
[21] [assignment: list of cryptographic operations]
[22] [assignment: cryptographic algorithm]
[23] [assignment: cryptographic key sizes]
[24] [assignment: list of standards]

FCS_COP.1/SIG_VER Cryptographic Operation - Signature verification by travel document

FCS_COP.1.1/SIG_VER The TSF shall perform *digital signature verification*[25] in accordance with a specified cryptographic algorithm (i) *RSA as given in* Table 15 *and (ii) ECDSA as given in* Table 16[26] and cryptographic key sizes *of modulus bit lengths of 1024, 1280, 1536, 2048 and 3072 bits and public exponent bit lengths up to 32 bits for RSA and the bit lengths of the curve of 160, 192, 224, 256, 320, 384, 512 and 521 bits for ECDSA* [27] that meet the following: *PKCS#1[28], [29] for RSA and [27] for ECDSA*[28].

Table 15: RSA Algorithms for signature verification in Terminal Authentication

OID	Signature	Hash	Parameters
id-TA-RSA-v1-5-SHA-1	RSASSA-PKCS1-v1_5	SHA-1	N/A
id-TA-RSA-v1-5-SHA-256	RSASSA-PKCS1-v1_5	SHA-256	N/A
id-TA-RSA-v1-5-SHA-512	RSASSA-PKCS1-v1_5	SHA-512	N/A
id-TA-RSA-PSS-SHA-1	RSASSA-PSS	SHA-1	default
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

Table 16: ECDSA Algorithms for signature verification in Terminal Authentication

OID	Signature	Hash
id-TA-ECDSA-SHA-1	ECDSA	SHA-1
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256
id-TA-ECDSA-SHA-384	ECDSA	SHA-384
id-TA-ECDSA-SHA-512	ECDSA	SHA-512

Application Note 29: The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

Application Note 30: The composite TOE also supports elliptic curves of length 522 to 640 bits; however, these curves are out of scope for the certification.

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

Application Note 31: Following the BSI recommendations stated on the certification report of Crypto Library Cobalt on N7021 VA, RSA key lengths below 1976 bits and EC key lengths below 250 bits are out of context for the certification.

FCS_COP.1/CA_MAC Cryptographic Operation - MAC for CA protocol

FCS_COP.1.1/CA_MAC The TSF shall perform *secure messaging - message authentication code*[29] in accordance with a specified cryptographic algorithm *CMAC and Retail MAC*[30] and cryptographic key sizes *112 bits for Retail MAC, 128, 192 and 256 bits for CMAC* [31] that meet the following: *TR-03110 [16]*[32].

Application Note 32: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as travel document Manufacturer or Personalization Agent by means of the authentication mechanism.

FCS_RND.1 Quality metric for random numbers

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 [41]) as random source.

DRG.4.2 The RNG provides forward secrecy (as defined in [41]).

DRG.4.3 The RNG provides backward secrecy even if the current internal state is known (as defined in [41]).

DRG.4.4 The RNG provides enhanced forward secrecy on demand (as defined in [41]).

DRG.4.5 The internal state of the RNG is seeded by an PTRNG or class PTG.2 (as defined in [41]).

FCS_RND.1.2 The TSF shall provide *numbers* that meet

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

[29] [assignment: list of cryptographic operations]
[30] [assignment: cryptographic algorithm]
[31] [assignment: cryptographic key sizes]
[32] [assignment: list of standards]

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 [41]).

6.2.2 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorization data

FIA_AFL.1.1/PACE The TSF shall detect when 5 [33] unsuccessful authentication attempts occur related to *authentication attempts using the PACE password as shared password*[34].

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[35], the TSF shall *consecutively increase the response time of the TOE to the next authentication attempt using PACE passwords*[36].

Application Note 33: After 5 consecutive unsuccessful authentication attempts, the TOE waits for 0,65 secs before responding to the next authentication attempt. The values given here are the default values for the number of unsuccessful authentication attempts and the response time and they are reconfigurable in the manufacturing phase, step 5.

FIA_UID.1/PACE Timing of identification

FIA_UID.1.1/PACE The TSF shall allow

- *to establish the communication channel,*
- *carrying out the PACE Protocol according to [19],*
- *to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,*
- *to carry out the Chip Authentication Protocol v.1 according to TR-03110-1 [17],*
- *to carry out the Terminal Authentication Protocol v.1 according to TR-03110-1 [17]*[37]

[33] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[34] [assignment: list of authentication events]
[35] [selection: met, surpassed]
[36] [assignment: list of actions]

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

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

Application Note 34: The SFR FIA_UID.1/PACE covers the definition in the EAC PP and extends the definition in the PACE PP.

Application Note 35: In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The eMRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the eMRTD”. The users in role “eMRTD Manufacturer” or “Personalization Agent” identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE, i.e., the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization Agent Key).

Application Note 36: User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ/Document Number effectively represent secrets, but are restricted revealable; i.e., it is either the travel document holder itself or an authorized other person or device (Basic Inspection System with PACE).

FIA_UAU.1/PACE Timing of authentication

FIA_UAU.1.1/PACE The TSF shall allow

- *to establish the communication channel,*
- *carrying out the PACE Protocol according to [19],*
- *to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,*
- *to identify themselves by selection of the authentication key,*

37 [assignment: list of TSF-mediated actions]

- *to carry out the Chip Authentication Protocol Version 1 according to TR-03110-1 [17],*
- *to carry out the Terminal Authentication Protocol Version 1 according to TR-03110-1 [17]* [38]

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

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

Application Note 37: The SFR FIA_UAU.1/PACE covers the definition in the EAC PP and extends the definition in the PACE PP.

Application Note 38: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e., it is either the travel document holder itself or an authorized other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}), cf. FTP_ITC.1/PACE.

FIA_UAU.4/PACE Single Use Authentication Mechanisms - Single-use authentication of the Terminal by the TOE

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

- *PACE protocol according to [19],*
- *Symmetric authentication mechanism based on AES 256,*
- *Asymmetric Authentication Mechanism based on RSA (activation agent),*
- *Terminal Authentication Protocol v.1 according to [17]*[39]*.*

FIA_UAU.5/PACE Multiple Authentication Mechanisms

FIA_UAU.5.1/PACE The TSF shall provide

- *PACE Protocol according to [19],*
- *Passive Authentication according to [12],*
- *Secure messaging in MAC-ENC mode according to [19],*
- *Symmetric Authentication Mechanism based on AES 256,*
- *Terminal Authentication Protocol v.1 according to [17]*[40]*,*

[38] [assignment: list of TSF mediated actions]
[39] [assignment: identified authentication mechanism(s)]

to support user authentication.

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

- *Having successfully run the PACE protocol, the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol,*
- *The TOE accepts the authentication attempt as Personalization Agent by* the Authentication Mechanism with Personalization Agent Keys*,*
- *After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1,*
- *The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1* [41]*.*

Application Note 39: The authentication of the Personalization Agent is based on the symmetric authentication mechanism with AES keys of 256 bits.

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

FIA_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions *each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal*[42].

Application Note 40: The PACE protocol specified in [19] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The

[40] [assignment: list of multiple authentication mechanisms]

[41] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

[42] [assignment: list of conditions under which re-authentication is required]

TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

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

FIA_UAU.6.1/EAC The TSF shall re-authenticate the user under the conditions *each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System*[43].

Application Note 41: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [12] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

FIA_API.1 Authentication Proof of Identity by Chip Authentication

FIA_API.1.1 The TSF shall provide a *Chip Authentication Protocol Version 1 according to [17]*[44] to prove the identity of the *TOE*[45].

Application Note 42: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [17]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [12]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

[43] [assignment: list of conditions under which re-authentication is required]
[44] [assignment: authentication mechanism]
[45] [assignment: authorized user or role]

6.2.3 CLASS FDP: USER DATA PROTECTION

FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the *Access Control SFP*[46] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document[47].

FDP_ACF.1/TRM Security attribute based access control

FDP_ACF.1.1/TRM The TSF shall enforce the *Access Control SFP*[48] to objects based on the following:

Subjects:

- *Terminal (1a),*
- *BIS-PACE (1b),*
- *Extended Inspection System (1c),*

Objects:

- *data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document (2a),*
- *fingerprint data stored in EF.DG3 of the logical travel document (2b),*
- *iris data stored in EF.DG4 of the logical travel document (2c),*
- *all TOE intrinsic secret cryptographic keys stored in the travel document (2d)*[49].

Security Attributes:

- *PACE Authentication (3a)*
- *Terminal Authentication v.1 (3b),*
- *Authorization of the Terminal (3c)*[50]

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *A BIS-PACE is allowed to*

[46] [assignment: access control SFP]
[47] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[48] [assignment: access control SFP]
[49] e.g. Chip Authentication Version 1 and ephemeral keys
[50] [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]

read data objects from FDP_ACF.1.1/TRM according to [19] after a successful PACE authentication as required by FIA_UAU.1/PACE [51].

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none* [52].

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

- *Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document,*
- *Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document,*
- *Any terminal being not successfully authenticated as Extended Inspection System with the Read access to EF.DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM,*
- *Any terminal being not successfully authenticated as Extended Inspection System with the Read access to EF.DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM,*
- *Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM,*
- *Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4*[53].

Application Note 43: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [16]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

[51] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[52] [assignment: rules, based on security attributes that explicitly authorise access of subjects to objects]
[53] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[54] the following objects:

- *Session Keys (immediately after closing related communication session) ,*
- *the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K[55])[56]*
- *none.*

FDP_UCT.1/TRM Basic Data Exchange Confidentiality - MRTD

FDP_UCT.1.1/TRM The TSF shall enforce the *Access Control SFP*[57] to be able to transmit and receive[58] user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/TRM Data Exchange Integrity

FDP_UIT.1.1/TRM The TSF shall enforce the *Access Control SFP*[59] to be able to transmit and receive[60] user data in a manner protected from modification, deletion, insertion and replay[61] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[62] has occurred.

6.2.4 CLASS FTP: TRUSTED PATH/CHANNELS

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[54] [selection: allocation of the resource to, deallocation of the resource from]
[55] according to [19]
[56] [assignment: list of objects]
[57] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[58] [selection: transmit, receive]
[59] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[60] [selection: transmit, receive]
[61] [selection: modification, deletion, insertion, replay]
[62] [selection: modification, deletion, insertion, replay]

FTP_ITC.1.2/PACE The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE The TSF shall **~~initiate~~ enforce** communication via the trusted channel for *any data exchange between the TOE and the Terminal*[63].

Application Note 44: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to "enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

Application Note 45: The trusted channel is established after successfully performing the Chip Authentication protocol or the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}); If the Chip Authentication protocol was successfully performed, secure messaging is immediately restarted using the derived session keys. This secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

6.2.5 CLASS FAU: SECURITY AUDIT

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide the *Manufacturer*[64] with the capability to store *the Initialization and Pre-Personalization Data*[65] in the audit records.

Application Note 46: The Manufacturer role is the default user identity assumed by the TOE in the life cycle Phase 2 Manufacturing. The IC manufacturer and the travel document Manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF-Data into the TOE. The audit records are write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).

[63] [assignment: list of functions for which a trusted channel is required]
[64] [assignment: authorised users]
[65] [assignment: list of audit information]

6.2.6 CLASS FMT: SECURITY MANAGEMENT

FMT_SMF.1 Specification of Management Functions

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

- *Initialization,*
- *Pre-personalization,*
- *Personalization,*
- *Configuration.*[66]

FMT_SMR.1/PACE Security Roles

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- *Manufacturer,*
- *Personalization Agent,*
- *Terminal,*
- *PACE authenticated BIS-PACE,*
- *Country Verifying Certification Authority,*
- *Document Verifier,*
- *Domestic Extended Inspection System,*
- *Foreign Extended Inspection System*[67]*.*

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

FMT_LIM.1 Limited capabilities

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

Deploying test features after TOE delivery does not allow

- *User Data to be manipulated and disclosed,*
- *TSF data to be manipulated and disclosed,*
- *software to be reconstructed,*

[66] **[**assignment: list of management functions to be provided by the TSF]
[67] [assignment: the authorised identified roles]

- *substantial information about construction of TSF to be gathered which may enable other attacks and*
- *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.*[68]

FMT_LIM.2 Limited availability

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

- *User Data to be manipulated and disclosed,*
- *TSF data to be manipulated and disclosed,*
- *Software to be reconstructed,*
- *Substantial information about construction of TSF to be gathered which may enable other attacks,*
- *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.*[69]

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

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write[70] the *Initialization Data and Pre-personalization Data*[71] to *the Manufacturer*[72].

Application Note 47: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to read out[73] the *Initialization Data and the Pre-personalisation Data*[74] to *the Personalization Agent*[75].

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

Application Note 48: According to P.Manufact the IC Manufacturer and the travel document Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer.

The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes the IC Identifier as required by FAU_SAS.1.

The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization”. The external read access is blocked in the Phase 4 “Operational Use” since it is not needed and may be misused in the Phase 4. The travel document Manufacturer will write the Pre-personalization Data which is the personalization key.

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[76] the

- *PACE passwords,*
- *Chip Authentication Private Key,*
- *Personalization Agent Key*[77]

to *none*[78].

FMT_MTD.1/PA Management of TSF data – Personalization Agent

FMT_MTD.1.1/PA The TSF shall restrict the ability to write[79] the *Document Security Object (SO$_D$)*[80] to the *Personalization Agent*[81].

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

FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[82] the

- *initial Country Verifying Certification Authority Public Key,*
- *initial Country Verifying Certification Authority Certificate,*
- *initial Current Date,*
- *none*[83]

to the *Personalization Agent*[84].

Application Note 49: The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update[85] the

- *Country Verifying Certification Authority Public Key,*
- *Country Verifying Certification Authority Certificate*[86]

to *Country Verifying Certification Authority*[87].

Application Note 50: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates [17]. The TOE updates its internal trust-point if a valid Country Verifying CA Link- Certificates (cf. FMT_MTD.3) is provided by the terminal [17].

FMT_MTD.1/DATE Management of TSF data – Current date

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify[88] the *current date*[89] to

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

- *Country Verifying Certification Authority,*
- *Document Verifier,*
- *Domestic Extended Inspection System*[90]*.*

Application Note 51: The authorized roles are identified in their certificate (ref [17] sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (ref [17], annex A.3.3, for details).

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *load*[91] the *Chip Authentication Private Key*[92] to *the Personalization Agent*[93].

FMT_MTD.1/KEY_CHANG Management of TSF data – Key Change

FMT_MTD.1.1/KEY_CHANG The TSF shall restrict the ability to change[94] the *Personalization Agent Keys*[95] to Manufacturer and Personalization Agent[96].

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for *TSF data of the Terminal Authentication Protocol v.1 and the Access Control*[97].

Refinement: The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not**

[90] [assignment: the authorised identified roles]
[91] [selection: create, load]
[92] [assignment: list of TSF data]
[93] [assignment: the authorised identified roles]
[94] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[95] [assignment: list of TSF data]
[96] [assignment: the authorised identified roles]
[97] [assignment: list of TSF data]

before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,

3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.**

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

6.2.7 CLASS FPT: PROTECTION OF THE TSF

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution*[98] in excess of *non-useful information*[99] enabling access to

1. *Chip Authentication Session Keys,*
2. *PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),*
3. *the ephemeral private key ephem-SK_{PICC}-PACE,*
4. *Personalization Agent Key(s)*,
5. *Chip Authentication Private Key*[100] *and*
6. Activation Agent Private Key[101]

FPT_EMS.1.2 The TSF shall ensure *any users*[102] are unable to use the following interface *smart card circuit contacts* [103] to gain access to

1. *Chip Authentication Session Keys,*
2. *PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC}),*

[98] [assignment: types of emissions]
[99] [assignment: specified limits]
[100] [assignment: list of types of TSF data]
[101] [assignment: list of types of user data]
[102] [assignment: type of users]
[103] [assignment: type of connection]

3. *the ephemeral private key ephem-SK_{PICC}-PACE,*
4. *Personalization Agent Key(s) and*
5. *Chip Authentication Private Key*[104] *and*
6. *Activation Agent Private Key*[105]

FPT_FLS.1 Failure with Preservation of Secure State

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

- *exposure to operating conditions causing a TOE malfunction,*
- *failure detected by TSF according to FPT_TST.1*,
- *none*[106].

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

Application Note 52: Secure state called security reset for TOE.

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, at the conditions *that critical commands are sent to the TOE*[107] to demonstrate the correct operation of the TSF[108].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF Data[109].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[110].

Application Note 53: Since the travel document's chip uses state of the art smart card technology, it will run the some self tests at the request of the authorized user and some self tests automatically. For instance, a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorized user" Manufacturer in the

[104] [assignment: list of types of TSF data]
[105] [assignment: list of types of user data]
[106] [assignment: list of types of failures in the TSF]
[107] [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]]
[108] [selection: [assignment: parts of TSF], the TSF]
[109] [selection: [assignment: parts of TSF data], TSF data]
[110] [selection: [assignment: parts of TSF], TSF]

Phase 2 Manufacturing. Other self tests may run automatically to detect failure and to preserve of secure state according to FPT_FLS.1 in the Phase 4 “Operational Use”.

FPT_PHP.3 Resistance to Physical Attack

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[111] to the *TSF*[112] by responding automatically such that the SFRs are always enforced.

Application Note 54: The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

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 is EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2.

[111] [assignment: physical tampering scenarios]
[112] [assignment: list of TSF devices/elements]

6.4 SECURITY REQUIREMENTS DEPENDENCIES

6.4.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

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

Table 17: Dependency of Composite TOE SFRs

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
1.	FAU_SAS.1	None	---
2.	FCS_CKM.1/DH_PACE	--- FCS_CKM.2 or FCS_COP.1 --- FCS_CKM.4	--- Not fulfilled but justified. See Explanation 1 --- FCS_CKM.4
3.	FCS_CKM.1/CA	--- FCS_CKM.2 or FCS_COP.1 --- FCS_CKM.4	--- FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC --- FCS_CKM.4
4.	FCS_CKM.4	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	--- FCS_CKM.1/DH_PACE, FCS_CKM.1/CA
5.	FCS_COP.1/PACE_ENC	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/DH_PACE --- FCS_CKM.4
6.	FCS_COP.1/CA_ENC	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/CA --- FCS_CKM.4
7.	FCS_COP.1/PACE_MAC	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/DH_PACE --- FCS_CKM.4
8.	FCS_COP.1/CA_MAC	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	--- FCS_CKM.1/CA --- FCS_CKM.4
9.	FCS_COP.1/SIG_VER	--- FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 --- FCS_CKM.4	---FCS_CKM.1/CA --- FCS_CKM.4

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
10.	FCS_RND.1	None	---
11.	FIA_UID.1/PACE	None	---
12.	FIA_UAU.1/PACE	--- FIA_UID.1	--- FIA_UID.1/PACE
13.	FIA_UAU.4/PACE	None	---
14.	FIA_UAU.5/PACE	None	---
15.	FIA_UAU.6/PACE	None	---
16.	FIA_UAU.6/EAC	None	---
17.	FIA_AFL.1/PACE	--- FIA_UAU.1	--- FIA_UAU.1/PACE
18.	FIA_API.1	None	---
19.	FDP_ACC.1/TRM	--- FDP_ACF.1	--- FDP_ACF.1/TRM
20.	FDP_ACF.1/TRM	--- FDP_ACC.1 --- FMT_MSA.3	--- FDP_ACC.1/TRM --- Not fulfilled but justified. See Explanation 2
21.	FDP_UCT.1/TRM	--- FTP_ITC.1 or FTP_TRP.1 --- FDP_ACC.1 orFDP_IFC.1	--- FTP_ITC.1/PACE --- FDP_ACC.1/TRM
22.	FDP_UIT.1/TRM	--- FDP_ACC.1 or FDP_IFC.1 --- FTP_ITC.1 or FTP_TRP.1	--- FDP_ACC.1/TRM --- FTP_ITC.1/PACE
23.	FDP_RIP.1	None	---
24.	FMT_SMF.1	None	---
25.	FMT_SMR.1/PACE	--- FIA_UID.1	--- FIA_UID.1/PACE
26.	FMT_LIM.1	--- FMT_LIM.2	--- FMT_LIM.2
27.	FMT_LIM.2	--- FMT_LIM.1	--- FMT_LIM.1
28.	FMT_MTD.1/INI_ENA	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
29.	FMT_MTD.1/INI_DIS	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
30.	FMT_MTD.1/CVCA_INI	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
31.	FMT_MTD.1/CVCA_UPD	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1

#	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
32.	FMT_MTD.1/DATE	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
33.	FMT_MTD.1/CAPK	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
34.	FMT_MTD.1/ PA	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
35.	FMT_MTD.1/KEY_READ	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
36.	FMT_MTD.1/KEY_CHANG	--- FMT_SMR.1 --- FMT_SMF.1	--- FMT_SMR.1/PACE --- FMT_SMF.1
37.	FMT_MTD.3	--- FMT_MTD.1	--- FMT_MTD.1/CVCA_INI, --- FMT_MTD.1/CVCA_UPD
38.	FTP_ITC.1/PACE	None	---
39.	FPT_EMS.1	None	---
40.	FPT_FLS.1	None	---
41.	FPT_PHP.3	None	---
42.	FPT_TST.1	None	---

Explanation 1: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

Explanation 2: The access control TSF according to FDP_ACF.1/TRM 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 EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 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 travel document's development and manufacturing especially for the secure handling of the travel document's material.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

All of these are met or exceeded in the EAL5 assurance package.

6.5 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The security objective **OT.Identification** "Identification of the TOE" addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data is defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: 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 SFR FMT_SMR.1/PACE lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/PA as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. When the Personalization Terminal authenticates itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key, the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Key. The SFR FMT_MTD.1/KEY_CHANG ensures that only the Personalization Agent can change the personalization key in the personalization mode. These two SFRs ensure together with the SFR FPT_EMS.1 the confidentially of the personalization key.

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for K_{enc}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy. The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA’s public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [5] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the

ENC_MAC_Mode secure messaging).The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure

- -by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- -by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- -by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:

(i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;

(ii) for listening to PACE communication (is of importance for the current PP, since SO_D is card-individual) – FTP_ITC.1/PACE.

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

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

Table 18: Coverage of TOE Objectives by SFRs

Security Functional Requirement	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1			✓				✓					
FCS_CKM.1/DH_PACE				✓	✓	✓						
FCS_CKM.1/CA	✓	✓	✓	✓	✓	✓						
FCS_CKM.4	✓		✓	✓	✓	✓						
FCS_COP.1/PACE_ENC						✓						
FCS_COP.1/CA_ENC	✓	✓	✓	✓		✓						
FCS_COP.1/PACE_MAC				✓	✓							
FCS_COP.1/CA_MAC	✓	✓	✓	✓								
FCS_COP.1/SIG_VER	✓		✓									
FCS_RND.1	✓		✓	✓	✓	✓						
FIA_AFL.1/PACE										✓		
FIA_UID.1/PACE	✓		✓	✓	✓	✓						
FIA_UAU.1/PACE	✓		✓	✓	✓	✓						
FIA_UAU.4/PACE	✓		✓	✓	✓	✓						
FIA_UAU.5/PACE	✓		✓	✓	✓	✓						
FIA_UAU.6/PACE				✓	✓	✓						
FIA_UAU.6/EAC	✓		✓	✓	✓	✓						
FIA_API.1		✓										
FDP_ACC.1/TRM	✓		✓	✓		✓						
FDP_ACF.1/TRM	✓		✓	✓		✓						

Security Functional Requirement	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FDP_RIP.1				✓	✓	✓						
FDP_UCT.1/TRM	✓			✓		✓						
FDP_UIT.1/TRM				✓		✓						
FMT_SMF.1		✓	✓	✓	✓	✓	✓					
FMT_SMR.1/PACE		✓	✓	✓	✓	✓	✓					
FMT_LIM.1								✓				
FMT_LIM.2								✓				
FMT_MTD.1/INI_ENA			✓				✓					
FMT_MTD.1/INI_DIS			✓				✓					
FMT_MTD.1/CVCA_INI	✓											
FMT_MTD.1/CVCA_UPD	✓											
FMT_MTD.1/DATE	✓											
FMT_MTD.1/CAPK	✓	✓		✓								
FMT_MTD.1/PA			✓	✓	✓	✓						
FMT_MTD.1/KEY_READ	✓	✓	✓	✓	✓	✓						
FMT_MTD.1/KEY_CHANG			✓									
FMT_MTD.3	✓											
FPT_EMS.1			✓						✓			
FPT_TST.1									✓			✓
FPT_FLS.1									✓			✓
FPT_PHP.3									✓		✓	

Security Functional Requirement	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FTP_ITC.1/PACE				✓	✓	✓				✓		

6.6 SECURITY ASSURANCE REQUIREMENTS RATIONALE

An assurance level of EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators shall have access to the detailed design knowledge and source code.

7 TOE SUMMARY SPECIFICATION

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

7.1 SF_PP: PHYSICAL PROTECTION

SF_PP, Physical Protection is mainly inherited from the Security IC part of composite product to AKIS GEZGIN_N. The Security Features inherited from the Security IC Platform are SF.OPC: Control of Operating Conditions, SF.PHY: Protection Against Physical Manipulation and SF.LOG: Logical Protection. For the security features fulfilled by Security IC, please see Security IC ST [5]. In addition, the SFR FPT_EMS.1 is included as a requirement for the ES part of the composite product and some Error Detection Code Control based features are added to the Embedded Software for FPT_PHP.3 requirement to enhance the protection of the access control files.

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

7.2 SF_DPM: DEVICE PHASE MANAGEMENT

Device phase management security feature is fulfilled by Security IC part of the composite product and the Embedded Software. The Security Feature inherited from the Security IC Platform is SF.COMP: Protection of Mode Control (for this security feature, please see Security IC ST [5]).

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

7.3 SF_AC: ACCESS CONTROL

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

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

The TOE restricts to write the personalization key to the **Activation Agent**. Once this key is written, the **Personalization Agent** has the right to change personalization key. No other roles are allowed to write or change this key. The **Personalization Agent** has the rights to create files and keys and to read files and public keys in the Personalization Phase.

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

- to enable/disable read access for users to the Initialization Data,
- to write the initial CVCA Public Key and the initial Current Date,
- to write the Chip Authentication Private Keys,
- to change the Personalization Agent key,
- to write and to read the data of the EF.COM, EF.SOD, EF.DGs of the logical MRTD after successful authentication.

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

The **Extended Inspection System** is the only role with Read access to Fingerprint and Iris data of the logical MRTD. In all other cases, reading any of these data is explicitly denied. Any other role including CVCA and DV is explicitly denied to read these data.

The **Country Verifying Certification Authority** has the ability to update the CVCA Public Key.

The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys, the Chip Authentication Private Key, the Personalization Agent Keys, and the Active Authentication Private Key.

Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.

No terminal is allowed

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

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 unauthorized modifications are possible.

Therefore, FAU_SAS.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3 SFRs are covered with Access Control Security feature.

7.4 SF_SM: SECURE MESSAGING

The TOE has SF_SM which allows the TOE to communicate to the external world securely. Secure Messaging feature protects the confidentiality, integrity and authenticity of the sensitive data exchanged between the TOE and the Inspection system.

After a successful SAC or Chip Authentication protocol, a secure channel is established based on Triple DES or AES algorithms.

This security functionality ensures

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

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

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

After a SAC or Chip Authentication protocol has been completed, the TOE rejects those commands that cause a failure of Secure Messaging.

Therefore, covered SFRs are: FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_CKM.4, FIA_UAU.6/PACE. FIA_UAU.6/EAC, FDP_RIP.1

7.5 SF_IA: IDENTIFICATION AND AUTHENTICATION

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

- Manufacturer and Personalization Agent authentication,
- PACE V2 protocol,
- Chip authentication mechanism of EAC,
- Terminal authentication mechanism of EAC

The eMRTD Manufacturer and the Personalization Agent authenticates themselves to the eMRTD by means of a mutual authentication mechanism based on AES algorithm. This feature detects each unsuccessful authentication attempt and after a certain number of unsuccessful authentication attempts blocks the related keys.

A BIS-PACE terminal may establish a secure messaging session The PACE-enabled Basic Access System and the eMRTD mutually authenticate by means of a PACE V2 protocol.

The eMRTD and the Inspection System perform a Diffie-Hellman (DH or ECDH) key agreement by means of keys derived from Document Number/MRZ or CAN. After a successful authentication, the generated session keys are independent of the entropy of this number. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way.

If eMRTD inspection is performed on a General Inspection System or an Extended Inspection System, then the MRTD's authenticity is proved executing the Chip Authentication Protocol. To this end two algorithms may be used: (i) a Diffie-Hellman key agreement compliant to PKCS #3 or ECDH key agreement compliant to ISO15946. Chip Authentication proves that the chip is genuine and also provides strong keys for Secure Messaging.

If eMRTD inspection is performed on an Extended Inspection System, then after a successful Chip Authentication the MRTD's chip recognizes that the Inspection System is entitled to access sensitive data, such as fingerprints, iris image and other role based data that are not easily available from other sources by means of the Terminal Authentication protocol

Terminal Authentication attempts are only accepted after a successful Chip Authentication and a consequent restart of the Secure Messaging session with the strong keys computed in the Chip Authentication.

The combination of Chip Authentication and Terminal Authentication provides an implementation of the Extended Access Control mechanism.

Therefore, the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_AFL.1/PACE, FCS_CKM.4, FIA_API.1/CA, FDP_RIP.1 are covered.

7.6 SECURITY FUNCTIONS RATIONALE

Table 19 shows the assignment of security functional requirements to TOE's security functionality.

Table 19: Coverage of SFRs by TOE Security Features

	Security Functional Requirement	SF_PP	SF_DPM	SF_AC	SF_SM	SF_IA
1.	FAU_SAS.1		✓			
2.	FCS_CKM.1/DH_PACE				✓	
3.	FCS_CKM.1/CA				✓	
4.	FCS_CKM.4				✓	
5.	FCS_COP.1/PACE_ENC				✓	
6.	FCS_COP.1/CA_ENC				✓	
7.	FCS_COP.1/PACE_MAC				✓	
8.	FCS_COP.1/CA_MAC				✓	
9.	FCS_COP.1/SIG_VER					✓
10.	FCS_RND.1					✓
11.	FIA_UID.1/PACE					✓
12.	FIA_UAU.1/PACE					✓
13.	FIA_UAU.4/PACE					✓
14.	FIA_UAU.5/PACE					✓
15.	FIA_UAU.6/PACE					✓
16.	FIA_UAU.6/EAC					✓
17.	FIA_AFL.1/PACE					✓
18.	FIA_API.1					✓
19.	FDP_ACC.1/TRM			✓		
20.	FDP_ACF.1/TRM			✓		
21.	FDP_UCT.1/TRM			✓		
22.	FDP_UIT.1/TRM			✓		
23.	FDP_RIP.1			✓		
24.	FMT_SMF.1			✓		

	Security Functional Requirement	SF_PP	SF_DPM	SF_AC	SF_SM	SF_IA
25.	FMT_SMR.1/PACE			✓		
26.	FMT_LIM.1		✓	✓		
27.	FMT_LIM.2		✓	✓		
28.	FMT_MTD.1/INI_ENA			✓		
29.	FMT_MTD.1/INI_DIS			✓		
30.	FMT_MTD.1/CVCA_INI			✓		
31.	FMT_MTD.1/CVCA_UPD			✓		
32.	FMT_MTD.1/DATE			✓		
33.	FMT_MTD.1/CAPK			✓		
34.	FMT_MTD.1/PA			✓		
35.	FMT_MTD.1/KEY_CHANG			✓		
36.	FMT_MTD.1/KEY_READ			✓		
37.	FMT_MTD.3			✓		
38.	FTP_ITC.1/PACE			✓		
39.	FPT_EMS.1	✓				
40.	FPT_FLS.1	✓				
41.	FPT_PHP.3	✓				
42.	FPT_TST.1	✓				

8 ABBREVIATIONS AND DEFINITIONS

3DES: Triple DES

AES: Advanced Encryption Standard

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

APDU: Application Packet Data Unit

BIS: Basic Inspection System

CA: Chip Authentication

CPU: Central Processing Unit

CSCA: Country Signing Certification Authority

CVCA: Country Verifying Certification Authority

DES: Decryption and Encryption Standard

DFA: Differential Fault Analysis

DPA: Differential Power Analysis

EAC: Extended Access Control

EAL: Evaluation Assurance Level

EEPROM: Electrically Erasable Programmable Read Only Memory

EIS: Extended Inspection System

ES: Embedded Operating System

IC: Integrated Circuit

MRTD: Machine Readable Travel Document

MRZ: Machine Readable Zone

PACE: Password Authenticated Connection Establishment

PP: Protection Profile

PTG2: A class that defines the requirements for RNGs used in key generation, padding bit generation, etc. PTG.2 is defined AIS31 [40]

RAM: Random Access Memory

RSA: Ron Rivest, Adi Shamir and Leonard Adleman

ROM: Read Only Memory

SAC: Supplemental Access Control

SAM: Secure Access Module

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

9 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), BSI-CC-PP-0068-V2-2011, version 1.0, 2nd November 2011.

[5] NXP Secure Smart Card Controller N7021 VA Security Target Lite, Rev. 2.3, 2019-06-04.

[6] Crypto Library Cobalt on N7021 VA Security Target Lite, Rev. 2.3, 5 June 2019

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

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

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

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

MRTD specifications

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

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

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

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

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

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

[17] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1, eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012.

[18] Supplement to Doc 9303 – Release 11 – November 17, 2011

[19] Technical Report Supplemental Access Control For Machine Readable Travel Documents – version 1.01 – November 11, 2010

Standards

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009.

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

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

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

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

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

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

[27] American National Standard X9.62-2005: Public Key Cryptography For The Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.

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

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

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

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

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

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

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

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

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

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

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

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

Misc

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

[41] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011