TÜBİTAK BİLGEM UEKAE

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

e-ID Technologies Unit

SECURITY TARGET LITE

of

AKIS GEZGIN_N v2.0

SAC & EAC Configuration

Revision no	01
Revision date	16.02.2024
Document code	AKiS-GEZGiN_N-SAC-EAC-ST-Lite-01
Prepared by	Ali YILDIRIM

REVISION HISTORY

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: Security Target Lite of AKIS GEZGIN_N v2.0 SAC & EAC Configuration

Document Version: 01

CC Version: 3.1 (Revision 5)

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

1.2 TOE REFERENCE

The current Security Target refers to the product AKIS GEZGIN_N SAC & EAC Configuration. The short version number of the TOE is 2.0 and the full version number of the TOE is 2.0.0.7.

1.3 TOE OVERVIEW

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

In this document, both the terms “AKIS GEZGIN” and “AKIS GEZGIN_N” refer to “AKIS GEZGIN_N supporting Supplemental Access Control (SAC) mechanism, Extended Access Control (EAC) mechanism, and e-Sign application”.

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 (or IDL’s) chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software including operating system and eMRTD / IDL / e-Sign applications,
- activation data,
- guidance documentation with personalization recommendations.

1.3.1 TOE TYPE AND USAGES OF THE TOE

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

Supporting eMRTD, IDL and e-Sign applications, the TOE is a native software embedded in contactless smart card IC P71D352P of NXP N7121 P71D31 platform. During the manufacturing and personalization phases, the TOE can be configured to serve five different use cases: eMRTD, IDL, e-Sign, eMRTD along with e-Sign, and IDL along with e-Sign.

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

Additionally, the TOE provides PIN management and e-Signature services. There are two types of uses for PINs: (i) PINs created under MF for SAC (PACEv2) mechanism and (ii) PINs created under e-Sign application for the authorization required to use the private keys to generate e-Signatures.

Part 3 of ISO-compliant driving licence (IDL) standard ISO 18013 [29] includes support for subsets of EAC v1 and SAC (PACEv2) such that it only supports ECDH algorithms for SAC and EAC Chip Authentication v1 and ECDSA for EAC Terminal Authentication v1 (DH algorithms for SAC and EAC Chip Authentication v1 and RSA signature verification algorithms for EAC Terminal Authentication v1 are not supported).

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

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)	✓	✓

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),
- Hybrid Deterministic Random Number Generation,
- Signature generation with RSASSA-PKCS1-v1_5 and RSASSA-PSS,
- Signature generation with ECDSA.

1.3.3 NON-TOE HARDWARE/SOFTWARE/FIRMWARE REQUIRED BY 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 [23] and [24].
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 [11] is granted. To authenticate a terminal as a basic inspection system with PACE, Standard Inspection Procedure must be used.

1.4 TOE DESCRIPTION

1.4.1 LOGICAL SCOPE OF THE TOE

A logical TOE will have data of the TOE holder stored according to the Logical Data Structure as specified by ICAO Doc 9303 [10] for eMRTD and by ISO 18013-2 [28] for IDL on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the TOE holder.

- The digital MRZ[1] Data,
- The digitized portraits,
- The optional biometric reference data of finger(s) or iris image(s) or both,
- The other data according to Logical Data Structure and
- The Document security object.

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

1.4.1.1 LDS APPLICATION

The Logical Data Structure (LDS) application is a generic file system that can be configured to meet ICAO Doc 9303 e-Passport specifications [10] or ISO 18013 ISO-compliant Driving Licence specifications [28]. An optional e-Sign application is also supported.

The generic file system is given in the Figure 1.

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

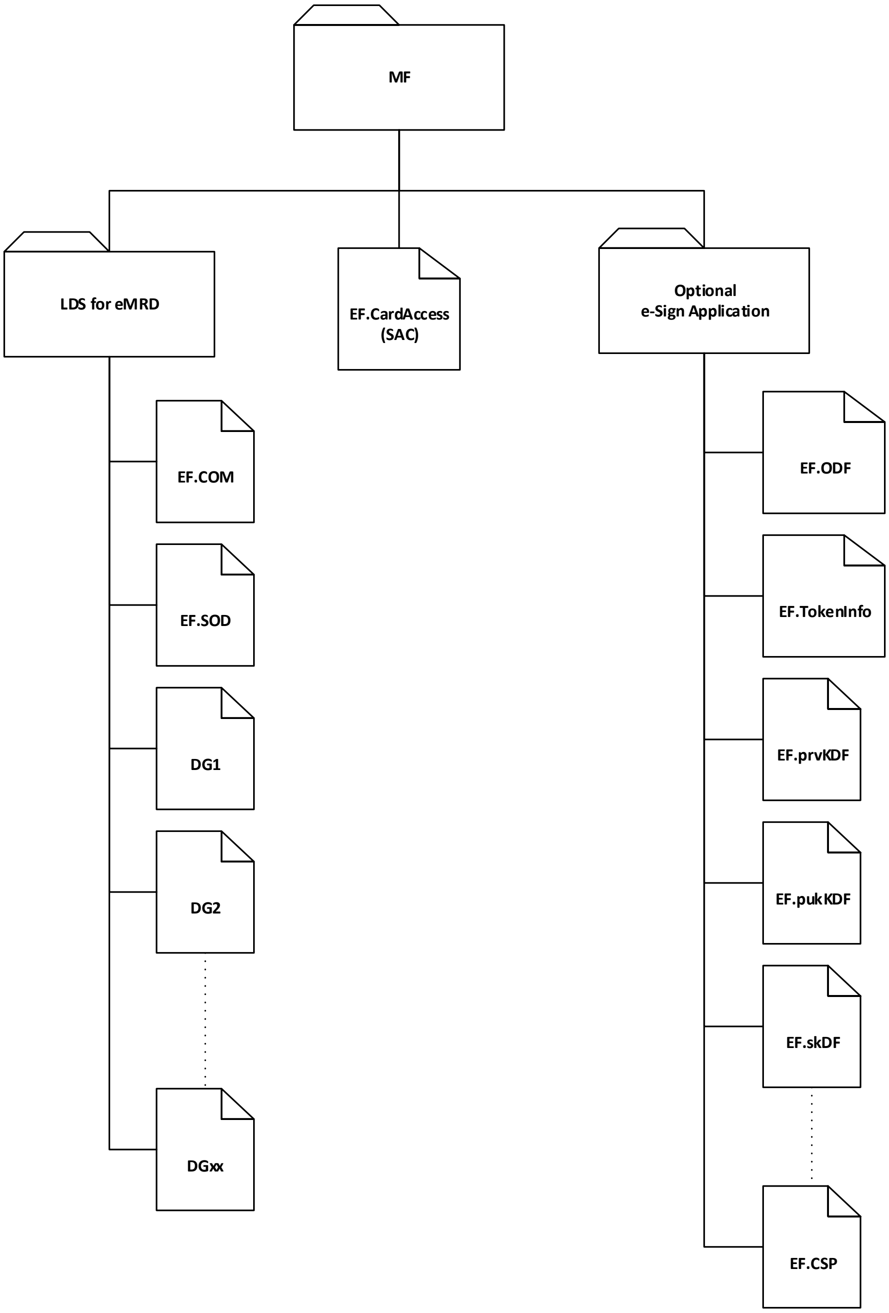


Figure 1: Generic file system of the TOE

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

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

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

1.4.1.1.1 SYSTEM FILES

System files are dedicated to store sensitive data that are used by the application. The integrity of the System Files is protected by means of a checksum. The system files used for MRD may be created and updated during the Personalization operation only; however, since the TOE also supports e-Signature generation, the data belonging to e-Sign application such as asymmetric private keys, public certificates, etc. may also be created, written and updated during the Operational Use phase as well. The keys stored in system files are not readable.

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

In particular, these files are used to store:

- EAC Chip Authentication Private Key,
- EAC Terminal Authentication Public Key,
- Asymmetric private keys for e-Signature generation.

1.4.1.1.2 DATA FILES

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

Common data files for MRD are as follows:

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

For the file structure under e-Sign application, please see PKCS #15 specification [19].

1.4.2 PHYSICAL SCOPE OF THE TOE

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

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

- The printed portrait.

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

The physical scope of the TOE is composed of the IC dedicated software, the IC embedded software and the IC platform that the embedded software runs on. Please see § 1.4.7 for more information on the IC platform.

The TOE comprises the following:

- the circuitry of the MRD's chip (contactless smartcard chip P71D352P of N7121 platform),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software including operating system and eMRTD/IDL/e-Sign applications,
- activation data,
- guidance documentation with personalization recommendations.

All components of the TOE are listed in Table 2.

Table 2: Components of the TOE

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

Document	AKIS GEZGIN_N v2.0 Kişiselleştirme Kılavuzu	5	DOC or PDF via hand-delivery
Document	AKIS GEZGIN_N v2.0 SAC & EAC Configuration Teslim ve İşletim Dokümanı	02	DOCX or PDF via hand-delivery
Activation data	N/A	N/A	Smartcard via hand-delivery or set of files via secure electronic delivery For details, see AKIS GEZGIN_N v2.0 SAC & EAC Configuration Teslim ve İşletim Dokümanı

1.4.3 SECURITY FEATURES OF THE TOE

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks mainly by platform specification and embedded operating system support as detailed in § 8,
- Passive Authentication (PA),
- Supplemental Access Control (SAC),
- Extended Access Control (EAC),
- The following cryptographic operations for e-Sign:
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Operations,
  - Signature generation with RSASSA-PKCS1-v1_5 and RSASSA-PSS,
  - Signature generation with ECDSA.

The hardware platform including the crypto library is certified for EAL 6 augmented and resistant to physical attacks. For details, please see the platform ST [5].

1.4.3.1 PASSIVE AUTHENTICATION (PA)

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

1.4.3.2 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 (and BAP Configuration 1), PACE is developed to prevent two types of attacks: skimming and eavesdropping.

The PACE Protocol, which is specified in [11], 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). When the TOE is 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 (or BAP Configuration 1, in the case of IDL).

Throughout this document, the term PACE refers to PACEv2.

1.4.3.3 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 and BAP Configuration 1.

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 EF.DG14. The personalization agent decides what key(s) to store in EF.DG14 based on governmental policies. The terminal reads EF.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 EF.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 MRD, 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 3 shall be used:

Table 3: 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 4 shall be used:

Table 4: 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 stored temporarily by the TOE. At the start of the certificate chain, the terminal selects the cryptographic key (either ECC or RSA Key), that was used for signing the first certificate of the chain, among the keys already stored in the TOE in EF.CVCA file.

The 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 it has already received in the certificate chain. 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.

1.4.4 INTERFACES

For the electrical I/O:

- ISO 1177 Information processing — Character structure for start/stop and synchronous character oriented transmission, 1985-07-25 [22],
- ISO 14443-3 Cards and security devices for personal identification — Contactless proximity objects, Part 3: Initialization and anticollision, Fourth edition, 2018-07 [23],
- ISO 14443-4 Cards and security devices for personal identification — Contactless proximity objects, Part 4: Transmission protocol, Fourth edition, 2018-07 [24].

For the commands:

- ISO 7816 Commands[2] [25], [26], [27]
- MRTD Commands [10], [13]
- IDL Commands [29]

[2] APDUs for e-Sign application are covered by ISO 7816 APDUs.

1.4.5 LIFE CYCLE

This Security Target is based on 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 this PP and given as follows. Note that any TOE-specific details are given in *italics*.

Phase-1: Development

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

Phase-2: Manufacturing

- **(Step3)** In a first step the TOE integrated circuit is produced containing the chip Dedicated Software and the parts of the MRD's chip Embedded Software in the non-volatile non-programmable memories. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRD material during the IC manufacturing and the delivery process to the MRD manufacturer. The IC is securely delivered from the IC manufacturer to the MRD manufacturer.
- If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance NVM)[3].
- **(Step4)** The MRD manufacturer combines the IC with hardware for the contactless interface in the MRD book*/card*.

[3] 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.

- **(Step5)** The MRD manufacturer (i) creates the MRTD/IDL application (create MF and LDS) and (ii) equips the chips with pre-personalization Data.
  - ***(Activation)*** *AKIS GEZGIN_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. When the TOE is sent the very first APDU, it checks the FabKey data: if the FabKey data does not match the expected value, the TOE enters the Death phase. Before the activation command, activation agent is to transfer activation public key, in the same session, to the TOE via PSO: VERIFY CERTIFICATE command. Managed by activation agent, this phase is ended by activation operation in which a 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*[4].
  - ***(Initialization)*** *After successful authentication of initialization key, another successful authentication is needed to complete this step. File structure is created during this step.*
- The pre-personalized MRD together with the IC Identifier is securely delivered from the MRD manufacturer to the Personalization Agent. The MRD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase-3: Personalization of the MRD

- ***(Step6)*** *This phase starts with the successful authentication of personalization key. Another successful authentication is needed to complete this phase. Personal information data are written and access rules are defined in this phase. Application specific restrictions cannot be implemented in personalization phase.*
- The personalization of the MRD includes (i) the survey of the MRD holder's biographical data, (ii) the enrolment of the MRD holder biometric reference data (i.e., the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable

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

data onto the physical MRD, (iv) the writing of the TOE User Data and TSF Data into the logical MRD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ[5] data (EF.DG1), (ii) the digitized portrait (EF.DG2 [6]), and (iii) the Document security object.

- The signing of the Document security object by the Document Signer finalizes the personalization of the genuine MRD for the MRD holder. The personalized MRD (together with appropriate guidance for the TOE use if necessary) is handed over to the MRD holder for operational use.

Phase-4: Operational Use

- **(Step7)** The TOE is used as MRD's chip by the user and the inspection systems in the "Operational Use" phase. The user data on eMRD can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State or Organization but they can never be modified. Since the TOE also supports e-Signature generation, the data belonging to e-Sign application such as asymmetric private keys, public certificates, etc. may also be created, written and updated during the Operational Use phase as well. The associated guidance documentation contains more detailed information about how and when these files may be created/updated.

Phase-5: Death Phase

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

[5] for eMRTD
[6] For IDL: EF.DG4

1.4.6 TOE CONFIGURATIONS

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

The TOE can be personalized for three types of applications: eMRTD, IDL, and e-Sign. The first and second applications are mutually exclusive, i.e., the TOE can be personalized to have only one of these two applications; however, the TOE can optionally be personalized to also have an e-Sign application either along with eMRTD / IDL application or independently.

1.4.7 PLATFORM INFORMATION

Platform:
NXP Technologies, N7121 P71D321

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

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

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

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

Common Criteria Version:
CC v3.1 Revision 5

2 CONFORMANCE CLAIM

2.1 CC CONFORMANCE CLAIM

This security target and the TOE claim conformance to

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

as follows:

- Part 2 extended,
- Part 3 conformant.

2.2 PP CLAIM

This ST is based on 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].

Since the TOE also supports e-Signature generation, new SFRs, in addition to those given in [3] and [4], are added to this ST.

2.3 PACKAGE CLAIM

The current ST is conformant to the following security requirements package: assurance package EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in CC part 3 [8].

2.4 CONFORMANCE CLAIM RATIONALE

Since the types of TOE defined in this ST (please see §1.3.1) and EAC PP [3] (please see §1.1) do not match, no strict conformance to EAC PP is claimed; instead, this ST is based on EAC PP.

An assurance level of EAL 5 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to have the capability to defend against sophisticated attacks.

3 SECURITY PROBLEM DEFINITION

The TOE is the composition of the security IC and the Embedded Software (ES) which includes the eMRTD/IDL/e-Sign applications. 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].

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

3.1 ASSETS

3.1.1 ASSETS PROTECTED BY THE eMRTD/IDL APPLICATION

Assets protected by the TOE are given in Table 5. These assets, applicable to both eMTRD and IDL, are protected against advanced attackers.

Table 5: Assets protected by the TOE

Primary Assets			
No	**Asset**	**Definition**	**Protected Against**
1.	User data stored on the TOE	All data (except authentication data) stored in the context of the eMRTD/IDL 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 MRD's chip, Logical MRD 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	All data (except authentication data) being transferred in the context of the eMRTD/IDL application of the travel document between the TOE and an authenticated terminal acting as Basic Inspection System with PACE.	Confidentiality Integrity Authenticity

	Inspection System 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 MRD 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
4.	Logical travel document sensitive User Data	Sensitive biometric reference data stored in data groups EF.DG3 [7] and EF.DG4 [8]	Confidentiality Integrity Authenticity
5.	Authenticity of the travel document's chip	The authenticity of the travel document's chip personalized by the issuing State or Organization for the MRD holder is used by the traveler to prove his or her possession of a genuine travel document.	Availability
Secondary Assets			
No	**Asset**	**Definition**	**Protected Against**
6.	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

[7] For IDL: EF.DG7
[8] For IDL: EF.DG8

7.	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 MRD's chip.	Availability
8.	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
9.	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
10.	Travel document communication establishment authorization data	Restricted-revealable authorization information for a human user being used 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.	Confidentiality Integrity

3.1.2 OTHER ASSETS

In addition to those mentioned above, the TOE may have the following assets in Table 6.

Table 6: Other assets protected by the TOE

No	Asset	Definition	Protected Against
1.	PINs	The TOE shall provide a PIN verification mechanism. As part of the PIN verification mechanism, PINs are	Confidentiality Integrity

		stored in containers that are provided by the TOE and transferred by the TSF mechanisms.	
2.	Private keys	The TOE shall provide containers to store and manage asymmetric private keys securely. Private keys are transferred to these containers by the TSF mechanisms.	Confidentiality Integrity
3.	Access Rules Reference (ARR) file	This is the file created to control access to the two assets given above and the TSF interface. The integrity need of this file is different from LDS data groups. Thus, it is regarded as a different asset.	Integrity

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
MRD holder	The rightful holder of the travel document for whom the MRD is personalized by the issuing State or Organization.
Traveler	A person presenting the travel document to a terminal and claiming the identity of the MRD holder.
Signatory	Person who holds the TOE and uses it on their behalf or on behalf of legal persons or entities that they represent for the purpose of creating e-Signatures.

Terminal	A terminal is any technical system communicating with the TOE through the contactless interface.
Inspection system (IS)	A technical system used by the control officer[9] 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 MRD holder. The **Basic Inspection System (BIS)** (i) contains a terminal for the contactless communication with the MRD’s chip, (ii) implements the terminals part of the BAC/BAP Mechanism and (iii) gets the authorization to read the logical MRD under the BAC/BAP by optical reading the MRD or other parts of the MRD 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 MRD holder (for eMRTD: by comparing the real biometric data -facial image- of the travel document presenter with the stored biometric data -EF.DG2- of the MRD holder) (for IDL: by comparing the real biometric data -facial image- of the travel document presenter with the stored biometric data -EF.DG4- of the IDL 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/BAP, (iii) gets the authorization to read the logical travel document either under PACE or BAC/BAP by optical reading the travel document providing this information, (iv) implements the Terminal Authentication protocol version 1 and Chip Authentication protocol version 1 according to [12] and (v) is authorized by the issuing State or Organization through the Document Verifier

[9] A border control officer of the receiving State or Organization who has got the authority to inspect eMRTD is the control officer whereas an official of the receiving Organization who has got the authority to inspect IDL is the control officer.

	of the receiving State or Organization to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC/BAP may only be used if supported by the TOE. If both PACE and BAC/BAP are supported by the TOE and the BIS, PACE must be used. The **Extended Inspection System with CVC Extensions (EIS-Authentication)** is similar to the Extended Inspection System (EIS) in that it also performs the Advanced Inspection Procedure; in addition, the TOE accepts certificate extensions only from EIS-Authentication terminals during the Terminal Authentication. The EIS-Authentication is authorized by the issuing State or Organization through the Document Verifier of the receiving State or Organization to read the data outside the context of eMRD. Security attributes of the EIS-Authentication are defined by means of the Authentication System Certificates.
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 MRD holder by some or all of the following activities: (i) establishing the identity of the MRD holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the MRD 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 MRD holder as defined in [11] for eMRTD ([29] for IDL), (iv) writing the document details data, (v) writing the initial TSF data and (vi) signing the Document Security Object defined in [11] for eMRTD ([29] for IDL). 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 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 MRD. 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 or Organization 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 MRD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
Attacker[10]	A threat agent trying (i) to undermine the security policies, especially to change properties of the assets having to be maintained, (ii) to manipulate

[10] 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.

	the logical travel document without authorization, (iii) to read sensitive biometric reference data (i.e., EF.DG3 and EF.DG4) [11], (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.

3.3 THREATS

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

[11] For IDL: EF.DG7 and EF.DG8.

Table 8: Hardware, terminal, communication and application related threats

No	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/SAI 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

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 eMRD
4.	T.Eavesdropping: Eavesdropping on the communication between the TOE and the PACE terminal	**Adverse action:** (i) 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. (ii) An attacker might also be listening to an existing communication between the MRD’s chip and an e-Signature terminal to capture the value(s) of PIN(s) used to authenticate for the use of asymmetric private keys to perform e-Signature generation operations. **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 (i) logical travel document data (ii) PINs
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 MRD holder

6.	T.Forgery: Forgery of data	**Adverse action:** An attacker fraudulently alters the User Data or/and TSF-data stored on the eMRD or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS PACE by means of changed MRD 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
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 MRD 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.
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
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
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's 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
11.	T.Unauthorised_Access_Sign_Key	**Adverse action:** An attacker may improperly use the asymmetric private keys used for e-Signature generation or may capture the value(s) of PIN(s) needed to authenticate for e-Signature generation using asymmetric private keys that he or she is not authorized to. It is assumed for the attack scenario to succeed that no secure communication was established between the terminal and the TOE before using asymmetric private keys to generate e-Signatures. The attacker then eavesdrops to the wireless communication between the terminal and the TOE to capture the value(s) of the PIN(s) needed for authentication. In addition, the software used for the generation of e-Signatures may, intentionally or inadvertently, direct TOE holders to sign additional documents without his or her knowledge or approval.

		Threat agent: having enhanced basic attack potential, not knowing the PIN(s) needed to authenticate for e-Signature generation **Asset:** value(s) of PIN(s), asymmetric private keys used for e-Signature generation
12.	T.Unauthorised_Management_Sign_Objects	**Adverse action:** An attacker may illegitimately use the security management services of the TOE for PINs and asymmetric private keys used for e-Signature generation. **Threat agent:** having basic attack potential, illegitimately attempting to manage PIN and asymmetric private key objects to be used for e-Signature generation **Asset:** PIN and asymmetric private key objects

3.4 ORGANISATIONAL SECURITY POLICIES

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

Table 9: Composite TOE Policies

No	Policy	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 eMRD 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 eMRD Issuer guarantees correctness of the user data (amongst other of those, concerning the MRD 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 MRD holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the eMRD Issuer's policy.

No	Policy	Definition
3.	P.Card_PKI: PKI for Passive Authentication (issuing branch)	**Application Note 1:** 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 eMRD 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 [11], § 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 [11], § 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.

No	Policy	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 MRD holders as defined in [11] for eMRTD ([29] for IDL). 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). 3. The related terminals need not to use any own credentials. 4. 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). 5. 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.

No	Policy	Definition
6.	P.Sensitive_Data: Privacy of sensitive biometric reference data	The biometric reference data of finger(s) (EF.DG3 [12]) and iris image(s) (EF.DG4 [13]) are sensitive private personal data of the MRD 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 or Organisations 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.
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 MRD holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.
8.	P.Access_Control_ Sign_Objects	Knowledge of PINs should be used as security attributes to determine the access control behavior and security management privileges during "operational-use" phase for PINs and asymmetric private keys used for e-Signature generation.

[12] For IDL: EF.DG7
[13] For IDL: EF.DG8

No	Policy	Definition
9.	P.Signature_Generation	The TOE shall support following e-Signature generation algorithms: • RSASSA-PKCS1-v1_5, • RSASSA-PSS, • ECDSA

3.5 ASSUMPTIONS

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

Table 10: Composite TOE Assumptions

No	Assumption	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 or Organisations 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

No	Assumption	Definition
		receiving States and Organizations. It is assumed that the Document Security Object contains only the hash values of the genuine user data.
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/BAP. BAC/BAP may only be used if supported by the TOE. If both PACE and BAC/BAP are supported by the TOE and the IS, PACE must be used. The EIS reads the logical eMRD under PACE or BAC/BAP and performs the Chip Authentication v.1 to verify the MRD 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 or Organisation 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. 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

No	Assumption	Definition
		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 Protocol Version 1.
4.	A.Sign_Keys: Cryptographic quality of asymmetric keys used for e-Signature generation	The asymmetric private keys used for e-Signature generation must provide sufficiently high cryptographic strength. High quality random numbers must be used for the generation of these key pairs.

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]. Since the TOE also supports e-Signature operations, three security objectives related to e-Signature operations have been added.

4.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.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 terminal connected (and represented by PACE authenticated BIS-PACE). 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 terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing: Tracing travel document

The TOE shall prevent gathering TOE tracing data by means of unambiguous identifying the eMRD 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,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

OT.Prot_Phys-Tamper: Protection against Physical Tampering

The TOE 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 electrical 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 (EF.DG3 and EF.DG4 for eMRTD; EF.DG7 and EF.DG8 for IDL) 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 eMRD 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 MRD's chip authenticity

The TOE shall support the Inspection Systems to verify the identity and authenticity of the MRD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication version 1 as defined in [12]. The authenticity proof provided by MRD's chip shall be protected against attacks with high attack potential.

Application Note 2: 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 [10][10] for eMRTD ([28] for IDL) and (ii) the hash value of EF.DG14 in the Document Security Object signed by the Document Signer.

OT.PIN_PrK_Management: Management of PINs and asymmetric private keys

The TOE must enable the management (creation, modification, and deletion) of PIN and asymmetric private key objects. These management functions must be performed by the authorized users only.

OT.Access_Control_Sign_Objects

The TOE must control the access to the user data and security services according to access control rules. Knowledge of PINs should be used as security attributes during the decision-making of whether access should be allowed.

OT.Signature_Generation

The TOE shall perform e-Signature generation operations.

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 eMRD. The storage of the Pre-Personalization data includes writing of the Personalization 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, before it is activated, in non-volatile memory for which all the security requirements of the platform are fulfilled.

OT.AC_Pers: Access Control for Personalization of logical MRD

The TOE shall ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document security object according to LDS [10] and the TSF data can be written by authorized Personalization Agents only. The logical 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.

In cases where the TOE is to be used as an IDL, the TOE shall ensure that the logical IDL document data in EF.DG1 to EF.DG14, the Document security object according to LDS [28] and the TSF data can be written by authorized Personalization Agents only. The logical travel document data in EF.DG1 to EF.DG14 and the TSF data may be written only during and cannot be changed after personalization of the document.

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

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

4.2.1 ISSUING STATE OR ORGANIZATION

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

OE.Legislative_Compliance: Issuing of the travel document

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

OE.Passive_Auth_Sign: Authentication of travel document by Signature

The travel document Issuer shall establish the necessary public key infrastructure as follows: 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 [11] for eMRTD ([29] for IDL). The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [11] for eMRTD ([29] for IDL). 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 its behalf (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 MRD 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 [11] for eMRTD ([29] for IDL), (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in ICAO Doc 9303 [11] for eMRTD ([29] for IDL) (in the role of a DS).

OE.Auth_Key_Travel_Document: Travel Document Authentication Key

The issuing State or Organisation shall 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 shall establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of MRD 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.MRD_Holder: MRD holder Obligations

The MRD 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 MRD holders as defined in [11] for eMRTD ([29] for IDL).
2. The related terminals implement the terminal parts of the PACE protocol [11] of the Passive Authentication [11] for eMRTD ([29] for IDL) (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, [11] for eMRTD ([29] for IDL)).
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.

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 [11] and/or the Basic Access Control [11] (or Basic Access Protection [29]). 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.

4.2.4 E-SIGNATURE GENERATION

The entities related to e-Signature generation will implement the following security objectives of the TOE environment.

OE.Cryptographic_Quality_Sign_Keys: Cryptographic quality of keys used for e-Signature generation

The entities creating asymmetric key pairs to be used for e-Signature generation, such as electronic signature service providers, must ensure that the keys generated must provide sufficiently high cryptographic strength.

OE.Proper_Signature_Software: Establishment of trusted channel before e-Signature creation

The entities developing software for creating e-Signatures must ensure that a trusted channel over PACEv2 is established first between a terminal and the TOE before any authentication, e.g., PIN verification, takes place for e-Signature generation.

4.3 SECURITY OBJECTIVES RATIONALE

The rationale between security objectives and threats, OSPs, and assumptions is given in Table 11.

Table 11: Security Objectives Rationale

	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	OT.PIN_PrK_Management	OT.Access_Control_Sign_Objects	OT.Signature_Generation	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.MRD_Holder	OE.Legislative_Compliance	OE.Cryptographic_Quality_Sign_Keys	OE.Proper_Signature_Software
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				
T.Unauthorised_Access_Sign_Key														X													X
T.Unauthorised_Management_Sign_Objects													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					
P.Access_Control_Sign_Objects													X													
P.Signature_Generation														X												
A.Insp_Sys																	X	X								
A.Auth_PKI																X			X							
A.Passive_Auth																	X				X					
A.Sign_Keys																									X	

Table 12: 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 reference data (EAC)	OT.Sens_Data_Conf OE.Authoriz_Sens_Data OE.Ext_Insp_Systems	The threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE objective **OT.Sens_Data_Conf** "Confidentiality of data" requiring that read access to DGs protected by EAC (containing sensitive biometric reference data) is only granted to authorized extended inspection systems. Furthermore it is required that the transmission of these data ensures the data 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 or Organisation has to authorize Extended Inspection

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
		Systems by creating appropriate Inspection System certificates for access to sensitive biometric 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 eMRD 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 MRD 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 eMRD.
T.Counterfeit: Counterfeit of MRD's chip (EAC)	OT.Chip_Auth_Proof, OE.Auth_Key_Travel_Document, OE.Exam_Travel_Document	The threat **T.Counterfeit** "Counterfeit of MRD's chip data" addresses the attack of unauthorized copy or reproduction of the genuine MRD's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of MRD's chip authentication" using an authentication key pair to be generated by the 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**

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
		"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 MRD'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-data or TSF-data as well as to disable or to bypass the soft-coded 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	
T.Malfunction: Malfunction due to Environmental Stress	OT.Prot_Malfunction	

Threats/OSPs/Assumptions	Corresponding Objectives	Rationale
T.Skimming: Skimming/Capturing Card-Terminal Communication	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OE.MRD_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.MRD_Holder** ensures that a PACE session can only be established either by the eMRD 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 MRD	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).
T.Unauthorised_Access_Sign_Key	OT.Access_Control_Sign_Objects	The threat **T.Unauthorised_Access_Sign_Key** addresses unauthorised access to data/assets. This threat is countered by the security objectives **OT.Access_Control_Sign_Objects** and **OE.Proper_Signature_Software** by ensuring only proper access to user data and security services.

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
T.Unauthorised_Management_Sign_Objects	OT.PIN_PrK_Management	The threat **T.Unauthorised_Management_Sign_Objects** addresses illegitimate use of the management services for PINs and asymmetric private keys. This threat is countered by the security objective **OT.PIN_PrK_Management** by ensuring that the use of these services are allowed for the authorized users only.
P.Manufact: Manufacturing of the MRD’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-data 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 objective **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).

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
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.
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 or Organisation 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 MRD 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 eMRD 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 MRD”. Note the IC Manufacturer equips the TOE with the eMRD manufacturer Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The eMRD Manufacturer equips the TOE with the Personalization Agent Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”.

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
P.Access_Control_Sign_Objects	OT.Access_Control_Sign_Objects	The OSP **P.Access_Control_Sign_Objects** states that knowledge of PINs may be used as security attributes to determine the access control behavior and security management privileges during “operational-use” phase. This OSP is implemented by the security objective **OT.Access_Control_Sign_Objects**.
P.Signature_Generation	OT.Signature_Generation	The OSP **P.Signature_Generation** requires the TOE to support e-Signature operations (namely RSASSA-PSS, RSASSA-PKCS1-v1_5, and ECDSA). This OSP is fulfilled by the security objective **OT.Signature_Generation**.
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 eMRD 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 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 MRD book/card addressed by the assumption A.Insp_Sys "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_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 MRD" will require the Inspection System to protect the logical MRD data during the transmission and the internal handling.

Threats/OSPs/Assumptions	**Corresponding Objectives**	**Rationale**
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 sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations only. The Document Verifier of the receiving State or 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 State or Organisation has to establish the necessary public key infrastructure.
A.Sign_Keys	OE.Cryptographic_Quality_Sign_Keys	The assumption A.Sign_Keys "Cryptographic quality of asymmetric keys used for e-Signature generation" is directly covered by the security objective for the TOE environment **OE.Cryptographic_Quality_Sign_Keys** "Cryptographic quality of keys used for e-Signature generation" ensuring the sufficiently high cryptographic strength to be provided by the entities creating asymmetric key pairs.

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.

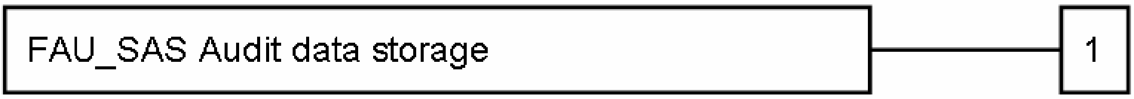
5.1 DEFINITION OF THE FAMILY FAU_SAS (AUDIT DATA STORAGE)

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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

5.1.1 FAU_SAS.1 AUDIT STORAGE

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FCS_RND of the Class FCS (cryptographic support) is defined in 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: Generation of random numbers
1

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*].

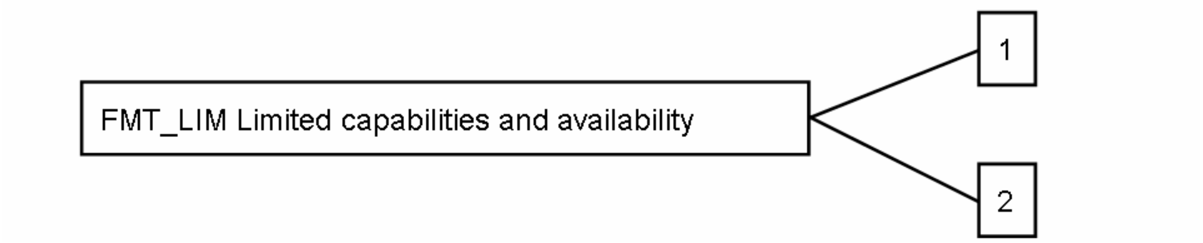
5.3 DEFINITION OF THE FAMILY FMT_LIM (Limited Capabilities And Availability)

FMT_LIM of the Class FMT (Security Management) is defined as given in 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.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.

Dependencies: FMT_LIM.2 Limited availability

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

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

5.3.2 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 Part 2.

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*].

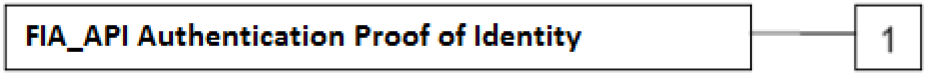
5.5 DEFINITION OF THE FAMILY FIA_API (AUTHENTICATION PROOF OF IDENTITY)

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 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 operations are defined in § 8.1 of Common Criteria Part 1 [6]. All these operations are used in this ST.

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

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

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

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

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

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

6.2 SECURITY FUNCTIONAL REQUIREMENTS

This ST is based on the protection profiles EAC PP [3] and PACE PP [4] and all the SFRs in these PP's are included in this security target. Since the TOE also supports e-Signature generation, the SFRs directly related to e-Signature are included here as well. In addition, the SFRs FDP_ACC.1 and FDP_ACF.1 are iterated for PINs.

TOE security functional requirements of the composite product are listed in Table 13.

Table 13: List of SFRs

SFR	Explanation
FCS_CKM.1/DH_PACE	Cryptographic Key Generation – Diffie-Hellman for PACE session

FCS_CKM.1/CA	Cryptographic Key Generation – Diffie-Hellman for Chip Authentication session keys
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/AUTH	Cryptographic Operation – Authentication
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/SIG_GEN	Cryptographic Operation – Signature generation
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_AFL.1/PIN	Authentication Failure Handling – PIN Verification
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_ACC.1/PIN	Subset access control – PIN Verification
FDP_ACF.1/TRM	Security attribute based access control
FDP_ACF.1/PIN	Security attribute based access control – PIN Verification

FDP_RIP.1	Subset residual information protection
FDP_UCT.1/TRM	Basic Data Exchange Confidentiality – MRD
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.1/PIN_Management	Management of TSF data – PINs
FMT_MTD.1/PrK_Management	Management of TSF data – Asymmetric Private Keys
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

Hierarchical to: No other components.

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

FCS_CKM.1.1/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 [14]*[14] and specified cryptographic key sizes *bit length of the modulus equal to 2048 and bit length of the exponent equal to or shorter than 2048 for (i) and 256, 384, 512 bits for (ii)*[15] that meet the following: *[11]*[16].

Application Note 3: The cryptographic functionality of the TOE includes DH operations with RSA keys of 1024 and 2048 bits and ECDH operations with ECC keys on elliptic curves brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, and brainpoolP512r1. However, due to additional platform crypto library restrictions for PACE, the certification of the TOE covers only the elliptic curves brainpoolP256r1, brainpoolP384r1, and brainpoolP512r1. In addition, RSA key lengths under 1976 bits are out of scope for the certification.

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on the (i) Diffie-Hellman key*

[14] [assignment: cryptographic key generation algorithm]
[15] [assignment: cryptographic key sizes]
[16] [assignment: list of standards]

derivation Protocol compliant to PKCS#3 [17] and (ii) ECDH compliant to [14][17] and specified cryptographic key sizes of *bit length for modulus 2048 bits for (i) and 224, 256, 320, 384, 512, and 521 bits for (ii)*[18] that meet the following: *[17] and [12] for (i) and [14] for (ii)*[19].

Application Note 4: The cryptographic functionality of the TOE includes DH operations with RSA keys of 1024 and 2048 bits and ECDH operations with ECC keys of 128-to-640 bits. However, due to security considerations and BSI recommendations (see the security target of the platform), certification of the platform covers standard elliptic curves ansix9p224r1, ansix9p256r1, ansix9p384r1, ansix9p521r1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, and ANSSI FRP256v1. As a consequence, the certification of the TOE covers only these elliptic curves as well. In addition, RSA key lengths under 1976 bits are out of scope for the certification.

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *secure erasing of the key value*[20] that meets the following: *none*[21].

[17] [assignment: cryptographic key generation algorithm]
[18] [assignment: cryptographic key sizes]
[19] [assignment: list of standards]
[20] [assignment: cryptographic key destruction method]
[21] [assignment: list of standards]

FCS_COP.1/AUTH Cryptographic Operation - Authentication

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH The TSF shall perform *symmetric authentication - encryption and decryption*[22] in accordance with a specified cryptographic algorithm *AES in CBC mode*[23] and cryptographic key sizes *256 bits*[24] that meet the following: *FIPS 197 [21], NIST SP 800-38A [20]*[25]**.**

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

Hierarchical to: No other components.

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

FCS_COP.1.1/PACE_ENC The TSF shall perform *secure messaging - encryption and decryption*[26] in accordance with a specified cryptographic algorithm *AES and Triple DES in CBC Mode*[27] and cryptographic key sizes *112 bits for 3DES and 128,192, and 256 bits for AES*[28] that meet the following: *[11]*[29]

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/PACE_MAC The TSF shall perform *secure messaging - message authentication code*[30] in accordance with a specified cryptographic algorithm *CMAC and Retail MAC*[31] and cryptographic key sizes *112 bits for Retail MAC and 128, 192, and 256 bits for CMAC*[32] that meet the following: *compliant to [11]*[33].

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or

FDP_ITC.2 Import of user data with security attributes or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/CA_ENC The TSF shall perform *secure messaging - encryption and decryption*[34] in accordance with a specified cryptographic algorithm *AES and 3DES in CBC mode*[35] and cryptographic key sizes *112 bits for 3DES and 128, 192, and 256 bits for AES*[36] that meet the following: *TR-03110-3, Annex E [13]*[37]

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or

FDP_ITC.2 Import of user data with security attributes or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SIG_VER The TSF shall perform *digital signature verification*[38] in accordance with a specified cryptographic algorithm *(i) RSA as given in Table 14 and (ii) ECDSA*

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

as given in Table 15 [39] and cryptographic key sizes *modulus bit lengths of 2048 and 3072 bits and public exponent bit lengths up to 32 bits for RSA and curve bit lengths of 224, 256, 320, 384, 512, and 521 bits for ECDSA*[40] that meet the following: *PKCS#1 [18] for RSA and [15] for ECDSA*[41].

Table 14: RSA Algorithms for signature verification in Terminal Authentication

OID	Signature	Hash	Parameters
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

Table 15: ECDSA Algorithms for signature verification in Terminal Authentication

OID	Signature	Hash
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 5: The cryptographic functionality of the TOE includes signature verification with RSA keys of 1024-to-3072 bits and ECDSA signature verification with ECC keys of 128-to-640 bits. However, due to security considerations and BSI recommendations (see the security target of the platform), certification of the platform covers standard elliptic curves ansix9p224r1, ansix9p256r1, ansix9p384r1, ansix9p521r1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, and ANSSI FRP256v1. As a consequence, the certification of the TOE covers only these elliptic curves as well. In addition, RSA key lengths under 1976 bits are out of scope for the certification.

Application Note 6: The cryptographic functionality of the TOE includes hash algorithm SHA-1. However, this algorithm is out of scope for the certification due to security considerations. The cryptographic functionality of the TOE also includes signature verification with RSASSA-PKCS1-v1_5

[39] [assignment: cryptographic algorithm]
[40] [assignment: cryptographic key sizes]
[41] [assignment: list of standards]

algorithm. However, due to security considerations, BSI and SOGIS recommendations (please see [31] and [32]) and the list of security mechanisms given in "ICAO Doc 9303" (please see [11]), this algorithm is out of scope for the certification as well.

FCS_COP.1/SIG_GEN Cryptographic Operation - Signature generation

Hierarchical to: No other components.

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

FCS_COP.1.1/SIG_GEN The TSF shall perform *digital signature generation*[42] in accordance with a specified cryptographic algorithm *(i) RSA as given in Table 16 and (ii) ECDSA as given in Table 17* [43] and cryptographic key sizes *modulus bit lengths of 1976 through 2560 bits for RSA and curve bit lengths of 224, 256, 320, 384, 512, and 521 bits for ECDSA*[44] that meet the following: *PKCS #1 [18] for RSA and [15] for ECDSA*[45].

Table 16: Algorithms used for signature generation with RSA

Signature	Hash
RSASSA-PSS	SHA-224
RSASSA-PSS	SHA-256
RSASSA-PSS	SHA-384
RSASSA-PSS	SHA-512

Table 17: Algorithms used for signature generation with ECDSA

Signature	Hash
ECDSA	SHA-224
ECDSA	SHA-256
ECDSA	SHA-384

[42] [assignment: list of cryptographic operations]
[43] [assignment: cryptographic algorithm]
[44] [assignment: cryptographic key sizes]
[45] [assignment: list of standards]

ECDSA	SHA-512

Application Note 7: The cryptographic functionality of the TOE includes signature generation with RSA keys of 1024-to-2560 bits and ECDSA signature generation with ECC keys of 128-to-640 bits. However, due to security considerations and BSI recommendations (see the security target of the platform), certification of the platform covers standard elliptic curves ansix9p224r1, ansix9p256r1, ansix9p384r1, ansix9p521r1, brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, and ANSSI FRP256v1. As a consequence, the certification of the TOE covers only these elliptic curves as well. In addition, RSA key lengths under 1976 bits are out of scope for the certification.

Application Note 8: The cryptographic functionality of the TOE includes hash algorithm SHA-1. However, this algorithm is out of scope for the certification due to security considerations. The cryptographic functionality of the TOE also includes signature generation with RSASSA-PKCS1-v1_5 algorithm. However, due to security considerations and BSI and SOGIS recommendations (please see [31] and [32]), this algorithm is out of scope for the certification as well.

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

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform *secure messaging - message authentication code*[46] in accordance with a specified cryptographic algorithm *CMAC and Retail MAC*[47] and cryptographic key sizes *112 bits for Retail MAC, 128, 192, and 256 bits for CMAC*[48] that meet the following: *TR-03110-3 [13]*[49].

FCS_RND.1 Quality Metric for Random Numbers

Hierarchical to: No other components.

[46] [assignment: list of cryptographic operations]
[47] [assignment: cryptographic algorithm]
[48] [assignment: cryptographic key sizes]
[49] [assignment: list of standards]

Dependencies: No dependencies.

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

DRG.4.1 The internal state of the RNG shall use PTRNG or class PTG.2 (as defined in [30]) as random source.

DRG.4.2 The RNG provides forward secrecy (as defined in [30]).

DRG.4.3 The RNG provides backward secrecy even if the current internal state is known (as defined in [30]).

DRG.4.4 The RNG provides enhanced forward secrecy on demand (as defined in [30]).

DRG.4.5 The internal state of the RNG is seeded by an PTRNG or class PTG.2 (as defined in [30]).

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

DRG.4.7 Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [30]).

6.2.2 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PACE The TSF shall detect when 5 [50] unsuccessful authentication attempts occur related to *authentication attempts using the PACE password as shared password*[51].

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[52], the TSF shall *consecutively increase the response time of the TOE to the next authentication attempt using PACE passwords*[53].

[50] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[51] [assignment: list of authentication events]
[52] [selection: met, surpassed]
[53] [assignment: list of actions]

FIA_AFL.1/PIN Authentication Failure Handling - PIN Verification

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PIN The TSF shall detect when an administrator configurable positive integer within *1 to 255* [54] unsuccessful authentication attempts occur related to *PIN authentication event*[55].

FIA_AFL.1.2/PIN When the defined number of unsuccessful authentication attempts has been met[56], the TSF shall *block the usage of PIN*[57].

FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE The TSF shall allow

- *to establish the communication channel,*
- *carrying out the PACE Protocol according to [11],*
- *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 [12],*
- *to carry out the Terminal Authentication Protocol v.1 according to TR-03110-1 [12],*
- *to verify PINs* [58]

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.

FIA_UAU.1/PACE Timing of authentication

Hierarchical to: No other components.

[54] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[55] [assignment: list of authentication events]
[56] [selection: met, surpassed]
[57] [assignment: list of actions]
[58] [assignment: list of TSF-mediated actions]

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/PACE The TSF shall allow

- *to establish the communication channel,*
- *carrying out the PACE Protocol according to [11],*
- *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,*
- *to carry out the Chip Authentication Protocol Version 1 according to TR-03110-1 [12],*
- *to carry out the Terminal Authentication Protocol Version 1 according to TR-03110-1 [12],*
- *to verify PINs*[59]

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.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *PACE protocol according to [11],*
- *Symmetric authentication mechanism based on AES 256,*
- *Asymmetric Authentication Mechanism based on RSA (activation agent),*
- *Terminal Authentication Protocol v.1 according to [12]*[60].

FIA_UAU.5/PACE Multiple Authentication Mechanisms

Hierarchical to: No other components.

[59] [assignment: list of TSF mediated actions]
[60] [assignment: identified authentication mechanism(s)]

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide

- *PACE Protocol according to [11],*
- *Passive Authentication according to [11]* [61]*,*
- *Secure messaging in MAC-ENC mode according to [11],*
- *Symmetric Authentication Mechanism based on AES 256,*
- *Terminal Authentication Protocol v.1 according to [12],*
- *PIN verification*[62]*,*

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* [63]*.*

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

Hierarchical to: No other components.

[61] [29] for IDL
[62] [assignment: list of multiple authentication mechanisms]
[63] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

Dependencies: No dependencies.

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*[64].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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*[65]*.*

FIA_API.1 Authentication Proof of Identity by Chip Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a *Chip Authentication Protocol Version 1 according to [12]*[66] to prove the identity of the *TOE*[67].

6.2.3 CLASS FDP: USER DATA PROTECTION

FDP_ACC.1/TRM Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/TRM The TSF shall enforce the *Access Control SFP*[68] on *terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document*[69].

FDP_ACC.1/PIN Subset access control – PIN verification

Hierarchical to: No other components.

[64] [assignment: list of conditions under which re-authentication is required]
[65] [assignment: list of conditions under which re-authentication is required]
[66] [assignment: authentication mechanism]
[67] [assignment: authorized user or role]
[68] [assignment: access control SFP]
[69] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/PIN The TSF shall enforce the *PIN Verification SFP*[70] on *signatories changing and unblocking PINs and creating e-Signatures over data to be signed*[71].

FDP_ACF.1/TRM Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/TRM The TSF shall enforce the *Access Control SFP*[72] 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 (for logical IDL data DGs, please see footnote*[73]*) (2a),*
- *fingerprint data stored in EF.DG3*[74] *of the logical travel document (2b),*
- *iris data stored in EF.DG4*[75] *of the logical travel document (2c),*
- *all TOE intrinsic secret cryptographic keys stored in the travel document (2d)*[76]

Security Attributes:

- *PACE Authentication (3a),*
- *Terminal Authentication v.1 (3b),*

[70] [assignment: access control SFP]
[71] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[72] [assignment: access control SFP]
[73] For IDL: EF.DG1 to EF.DG6 and EF.DG9 to EF.DG11
[74] For IDL: EF.DG7
[75] For IDL: EF.DG8
[76] e.g. Chip Authentication Version 1 and ephemeral keys as well as asymmetric private keys for e-Signature operations

- *Authorization of the Terminal (3c)*[77]

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 read data objects from FDP_ACF.1.1/TRM according to [11] after a successful PACE authentication as required by FIA_UAU.1/PACE*[78]*.*

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[79]*.*

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* [80] *(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* [81] *(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 (please see footnote*[82] *for IDL)*[83]*.*

[77] [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]
[78] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[79] [assignment: rules, based on security attributes that explicitly authorise access of subjects to objects]
[80] For IDL: EF.DG7
[81] For IDL: EF.DG8
[82] For IDL: the biometric data protected by EAC is in data groups EF.DG7 and EF.DG8
[83] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

Application Note 9: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [13]. 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.

FDP_ACF.1/PIN Security attribute based access control – PIN verification

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/PIN The TSF shall enforce the *PIN Verification SFP*[84] to objects based on the following:

Subjects:

- *Signatory*

Objects:

- *PINs,*
- *data to be signed*

Security attributes:

- *authentication status of signatories*[85]

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

- *the successfully authenticated Personalization Agent is allowed to create a template (including ARR files) of e-Sign application,*
- *the successfully authenticated Personalization Agent or Signatory is allowed to write and to read the data of the DGs of the e-Sign application,*
- *the successfully authenticated Signatory is allowed to perform e-Signature creation,*

[84] [assignment: access control SFP]

[85] [assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- *the successfully authenticated Signatory is allowed to change and unblock PINs*[86]*.*

FDP_ACF.1.3/PIN The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[87].

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

- *any user is not allowed to modify ARR files of the e-Sign application,*
- *any user is not allowed to modify any of the DGs of the e-Sign application,*
- *any user is not allowed to perform e-Signature creation,*
- *any user is not allowed to change and unblock PINs*[88]*.*

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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[89] 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*[90]*)*[91]*.*

FDP_UCT.1/TRM Basic Data Exchange Confidentiality – MRD

Hierarchical to: No other components.

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

[86] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[87] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[88] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[89] [selection: allocation of the resource to, deallocation of the resource from]
[90] according to [11]
[91] [assignment: list of objects]

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1/TRM The TSF shall enforce the *Access Control SFP*[92] to transmit and receive[93] user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/TRM Data Exchange Integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1/TRM The TSF shall enforce the A*ccess Control SFP*[94] to transmit and receive[95] user data in a manner protected from modification, deletion, insertion and replay[96] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[97] has occurred.

6.2.4 CLASS FTP: TRUSTED PATH/CHANNELS

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

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

[92] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[93] [selection: transmit, receive]
[94] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[95] [selection: transmit, receive]
[96] [selection: modification, deletion, insertion, replay]
[97] [selection: modification, deletion, insertion, replay]

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*[98].

6.2.5 CLASS FAU: SECURITY AUDIT

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide *the Manufacturer*[99] with the capability to store *the Initialization and Pre-Personalization Data*[100] in the audit records.

6.2.6 CLASS FMT: SECURITY MANAGEMENT

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *Initialization,*
- *Pre-personalization,*
- *Personalization,*
- *Configuration*[101].

FMT_SMR.1/PACE Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/PACE The TSF shall maintain the roles

- *Manufacturer,*
- *Personalization Agent,*
- *Terminal,*

[98] [assignment: list of functions for which a trusted channel is required]
[99] [assignment: authorised users]
[100] [assignment: list of audit information]
[101] **[**assignment: list of management functions to be provided by the TSF]

- *PACE authenticated BIS-PACE,*
- *Country Verifying Certification Authority,*
- *Document Verifier,*
- *Domestic Extended Inspection System,*
- *Foreign Extended Inspection System,*
- *signatory*[102]*.*

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

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

Deploying test features after TOE delivery does not allow

- *User Data to be manipulated and disclosed,*
- *TSF data to be manipulated and disclosed,*
- *software to be reconstructed,*
- *substantial information about construction of TSF to be gathered which may enable other attacks and*
- *sensitive User Data (EF.DG3 and EF.DG4)*[103] *to be disclosed*[104]*.*

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

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

Deploying test features after TOE delivery does not allow

[102] [assignment: the authorised identified roles]
[103] For IDL: EF.DG7 and EF.DG8
[104] [assignment: Limited capability and availability policy]

- *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)*[105] *to be disclosed*[106].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to *write*[107] the *Initialization Data and Pre-personalization Data*[108] to *the Manufacturer*[109].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to *read out*[110] the *Initialization Data and the Pre-personalization Data*[111] to *the Personalization Agent*[112].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

[105] For IDL: EF.DG7 and EF.DG8
[106] [assignment: Limited capability and availability policy]
[107] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[108] [assignment: list of TSF data]
[109] [assignment: the authorised identified roles]
[110] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[111] [assignment: list of TSF data]
[112] [assignment: the authorised identified roles]

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to *read*[113] the

- *PACE passwords,*
- *Chip Authentication Private Key,*
- *Personalization Agent Key,*
- *Asymmetric Private Keys*[114]

to *none*[115].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/PA The TSF shall restrict the ability to *write*[116] the *Document Security Object (SO_D)*[117] to *the Personalization Agent*[118].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to *write*[119] the

- *initial Country Verifying Certification Authority Public Key,*
- *initial Country Verifying Certification Authority Certificate,*
- *initial Current Date*[120]

to *the Personalization Agent*[121].

[113] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[114] [assignment: list of TSF data]
[115] [assignment: the authorised identified roles]
[116] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[117] [assignment: list of TSF data]
[118] [assignment: the authorised identified roles]
[119] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[120] [assignment: list of TSF data]
[121] [assignment: the authorised identified roles]

Application Note 10: 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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to *update*[122] the

- *Country Verifying Certification Authority Public Key,*
- *Country Verifying Certification Authority Certificate*[123]

to *Country Verifying Certification Authority*[124].

Application Note 11: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates [12]. The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal [12].

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/DATE	The TSF shall restrict the ability to modify[125] the *current date*[126] to

- *Country Verifying Certification Authority,*
- *Document Verifier,*
- *Domestic Extended Inspection System*[127].

[122] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[123] [assignment: list of TSF data]
[124] [assignment: the authorised identified roles]
[125] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[126] [assignment: list of TSF data]
[127] [assignment: the authorised identified roles]

Application Note 12: The authorized roles are identified in their certificate (ref [12] § 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 [12], annex A.3.3, for details).

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *load*[128] the *Chip Authentication Private Key*[129] to *the Personalization Agent*[130].

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_CHANG The TSF shall restrict the ability to *change*[131] the *Personalization Agent Keys*[132] to *Manufacturer and Personalization Agent*[133].

FMT_MTD.1/PIN_Management Management of TSF data – PINs

Hierarchical to: No other components.

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

FMT_MTD.1.1/PIN_Management The TSF shall restrict the ability to *write, change and unblock*[134] the *PIN objects*[135] to *the Personalization Agents and any application defined and allowed roles*[136].

[128] [selection: create, load]
[129] [assignment: list of TSF data]
[130] [assignment: the authorised identified roles]
[131] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[132] [assignment: list of TSF data]
[133] [assignment: the authorised identified roles]
[134] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[135] [assignment: list of TSF data]
[136] [assignment: the authorised identified roles]

FMT_MTD.1/PrK_Management Management of TSF data – Asymmetric Private Keys

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/PrK_Management	The TSF shall restrict the ability to *write and change*[137] the *asymmetric private key objects*[138] to *the Personalization Agents and any application defined and allowed roles*[139].

FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of 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*[140].

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 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.

[137] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[138] [assignment: list of TSF data]
[139] [assignment: the authorised identified roles]
[140] [assignment: list of TSF data]

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution*[141] in excess of *non-useful information*[142] 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,*
6. *Activation Agent Private Key,*
7. *Asymmetric Private Keys (e-Signature),*
8. *PINs*[143]

and

9. *EF.DG3 and EF.DG4 for eMRTD,*
10. *EF.DG7 and EF.DG8 for IDL*[144]

FPT_EMS.1.2 The TSF shall ensure *any users*[145] are unable to use the following interface *smart card circuit contacts* [146] to gain access to

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

[141] [assignment: types of emissions]
[142] [assignment: specified limits]
[143] [assignment: list of types of TSF data]
[144] [assignment: list of types of user data]
[145] [assignment: type of users]
[146] [assignment: type of connection]

3. *the ephemeral private key ephem-SK$_{PICC}$-PACE,*
4. *Personalization Agent Key(s),*
5. *Chip Authentication Private Key,*
6. *Activation Agent Private Key,*
7. *Asymmetric Private Keys (e-Signature),*
8. *PINs*[147]

and

9. *EF.DG3 and EF.DG4 for eMRTD,*
10. *EF.DG7 and EF.DG8 for IDL*[148]

FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- *exposure to operating conditions causing a TOE malfunction,*
- *failure detected by TSF according to FPT_TST.1* [149].

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

FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, at the conditions *that critical commands are sent to the TOE*[150] to demonstrate the correct operation of the TSF[151].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF Data[152].

[147] [assignment: list of types of TSF data]
[148] [assignment: list of types of user data]
[149] [assignment: list of types of failures in the TSF]
[150] [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]]
[151] [selection: [assignment: parts of TSF], the TSF]
[152] [selection: [assignment: parts of TSF data], TSF data]

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[153].

FPT_PHP.3 Resistance to Physical Attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[154] to the *TSF*[155] by responding automatically such that the SFRs are always enforced.

Application Note 13: 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 EAL 5 augmented with the following components:

- AVA_VAN.5 (Advanced methodical vulnerability analysis),
- ALC_DVS.2 (Sufficiency of security measures).

6.4 SECURITY REQUIREMENTS DEPENDENCIES

6.4.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

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

[153] [selection: [assignment: parts of TSF], TSF]
[154] [assignment: physical tampering scenarios]
[155] [assignment: list of TSF devices/elements]

Table 18: Dependency of Composite TOE SFRs

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
1.	FAU_SAS.1	None	
2.	FCS_CKM.1/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/AUTH	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— Not fulfilled but justified. See Explanation 4 — Not fulfilled but justified. See Explanation 4
6.	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
7.	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
8.	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
9.	FCS_COP.1/CA_MAC	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	— FCS_CKM.1/CA

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
		— FCS_CKM.4	— FCS_CKM.4
10.	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
11.	FCS_COP.1/SIG_GEN	— FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 — FCS_CKM.4	— Not fulfilled but justified. See Explanation 2 — Not fulfilled but justified. See Explanation 2
12.	FCS_RND.1	None	
13.	FIA_UID.1/PACE	None	
14.	FIA_UAU.1/PACE	— FIA_UID.1	— FIA_UID.1/PACE
15.	FIA_UAU.4/PACE	None	
16.	FIA_UAU.5/PACE	None	
17.	FIA_UAU.6/PACE	None	
18.	FIA_UAU.6/EAC	None	
19.	FIA_AFL.1/PACE	— FIA_UAU.1	— FIA_UAU.1/PACE
20.	FIA_AFL.1/PIN	— FIA_UAU.1	— FIA_UAU.1/PACE
21.	FIA_API.1	None	
22.	FDP_ACC.1/TRM	— FDP_ACF.1	— FDP_ACF.1/TRM
23.	FDP_ACC.1/PIN	— FDP_ACF.1	— FDP_ACF.1/PIN
24.	FDP_ACF.1/TRM	— FDP_ACC.1 — FMT_MSA.3	— FDP_ACC.1/TRM

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
			— Not fulfilled but justified. See Explanation 3
25.	FDP_ACF.1/PIN	— FDP_ACC.1 — FMT_MSA.3	— FDP_ACC.1/PIN — Not fulfilled but justified. See Explanation 5
26.	FDP_UCT.1/TRM	— FTP_ITC.1 or FTP_TRP.1 — FDP_ACC.1 or FDP_IFC.1	— FTP_ITC.1/PACE — FDP_ACC.1/TRM
27.	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
28.	FDP_RIP.1	None	
29.	FMT_SMF.1	None	
30.	FMT_SMR.1/PACE	— FIA_UID.1	— FIA_UID.1/PACE
31.	FMT_LIM.1	— FMT_LIM.2	— FMT_LIM.2
32.	FMT_LIM.2	— FMT_LIM.1	— FMT_LIM.1
33.	FMT_MTD.1/INI_ENA	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
34.	FMT_MTD.1/INI_DIS	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
35.	FMT_MTD.1/CVCA_INI	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
36.	FMT_MTD.1/CVCA_UPD	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1

No	Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
37.	FMT_MTD.1/DATE	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
38.	FMT_MTD.1/CAPK	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
39.	FMT_MTD.1/ PA	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
40.	FMT_MTD.1/KEY_READ	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
41.	FMT_MTD.1/KEY_CHANG	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
42.	FMT_MTD.1/PIN_Management	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
43.	FMT_MTD.1/PrK_Management	— FMT_SMR.1 — FMT_SMF.1	— FMT_SMR.1/PACE — FMT_SMF.1
44.	FMT_MTD.3	— FMT_MTD.1	— FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
45.	FTP_ITC.1/PACE	None	
46.	FPT_EMS.1	None	
47.	FPT_FLS.1	None	
48.	FPT_PHP.3	None	
49.	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 SFR FCS_COP.1/SIG_GEN uses asymmetric keys permanently stored during the Personalization phase. Since the keys are permanently stored within the TOE, there is no need for FCS_CKM.1 and FCS_CKM.4.

Explanation 3: 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.

Explanation 4: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus, there is no necessity to generate nor to import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE, there is no need for FCS_CKM.4, either.

Explanation 5: The access control TSF according to FDP_ACF.1/PIN uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e., FMT_MSA.3) is necessary here.

6.4.2 SECURITY ASSURANCE REQUIREMENTS DEPENDENCIES

The EAL 5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL 5 is applicable in those circumstances where a moderate to high level of independently assured security in conventional commodity TOEs are required.

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

The 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 EAL 5 assurance package.

6.5 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The security objective **OT.Identification** “Identification of the TOE” addresses the storage of Initialization and Pre-Personalization 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 Initialization and Pre-Personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalization Agent to disable access to Initialization and Pre-personalization 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 MRD” addresses the access control of the writing the logical MRD. The write access to the logical MRD 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 [156] of the logical MRD 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

[156] For IDL: EF.DG14

FCS_COP.1/AUTH (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The write access to the e-Sign application is defined by the SFRs FDP_ACC.1/PIN and FDP_ACF.1/PIN as follows: (i) only the successfully authenticated Personalization Agent is allowed to create a template (including ARR files) of the e-Sign application, (ii) only the successfully authenticated Personalization Agent or Signatory is allowed to write the data of the DGs of the e-Sign application.

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 Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 [157] 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 [158] 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 Personalization Agent only and, hence, is to be considered as trustworthy. The Personalization Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. The SFRs FCS_COP.1/AUTH, FIA_UAU.4/PACE, FIA_UAU.5/PACE, and FCS_CKM.4 represent some required specific properties of the protocols used (the authentication of the terminal as Personalization Agent shall be performed by TSF according to SFRs FIA_UAU.4/PACE and FIA_UAU.5/PACE using FCS_COP.1/AUTH). The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions (including Initialization and Personalization).

The write access to the data of the e-Sign application is defined by the SFRs FDP_ACC.1/PIN and FDP_ACF.1/PIN in the following way: (i) only the Personalization Agent is allowed to create a template (including ARR files) of the e-Sign application (FDP_ACF.1.2/PIN, rule 1), (ii) only the successfully

[157] For IDL: EF.DG14
[158] For IDL: EF.DG14

authenticated Personalization Agent or Signatory is allowed to write the data of the DGs of the e-Sign application (FDP_ACF.1.2/PIN, rule 2), (iii) no users are allowed to modify ARR files, and (iv) not authenticated users (users other than the successfully authenticated signatories) are not allowed to modify any of the data groups EF.DG1 to EF.DG14 of the e-Sign application, change and unblock PINs, or create e-Signatures (cf. FDP_ACF.1.4/PIN).

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 by unauthorized agents 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 data 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 K_{MAC}). 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 Personalization 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-data 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 Personalization 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 read access to the e-Sign application is defined by FDP_ACC.1/PIN and FDP_ACF.1.2/PIN: the successfully authenticated Personalization Agent or Signatory is allowed to read the data of the DGs of the e-Sign application.

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 [159] and EF.DG4 [160] 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

[159] For IDL: EF.DG7
[160] For IDL: EF.DG8

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 by unauthorized agents 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 updated 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 [12] 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 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 SFRs FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

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 PACE passwords (CAN, MRZ, SAI, PIN). This objective is achieved as follows:

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

(ii) for listening to PACE communication (is of importance for the current ST, 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.

The security objective **OT.PIN_PrK_Management** addresses illegitimate use of the management services for PINs and asymmetric private keys and ensures these management functions can be performed by authorized users only.

The security objective **OT.Access_Control_Sign_Objects** addresses user data protection against unauthorized access, through logical paths, to asymmetric private keys used for e-Signature creation. Physical paths are covered by OT.Prot_Phys-Tamper objective. The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE protect the user data from being accessed without identification and authentication. The SFRs FDP_ACC.1/PIN and FDP_ACF.1/PIN together require the enforcement of application access control policy.

The security objective **OT.Signature_Generation**, fulfilled by the SFR FCS_COP.1/SIG_GEN, addresses the need for e-Signature generation operations.

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

Table 19: 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	OT.PIN_PrK_Management	OT.Access_Control_Sign_Objects	OT.Signature_Generation
FAU_SAS.1			✓				✓								
FCS_CKM.1/DH_PACE				✓	✓	✓									
FCS_CKM.1/CA	✓	✓	✓	✓	✓	✓									
FCS_CKM.4	✓		✓	✓	✓	✓									
FCS_COP.1/AUTH			✓	✓											
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_COP.1/SIG_GEN															✓
FCS_RND.1	✓		✓	✓	✓	✓									
FIA_AFL.1/PACE										✓					
FIA_AFL.1/PIN							✓							✓	
FIA_UID.1/PACE	✓		✓	✓	✓	✓								✓	
FIA_UAU.1/PACE	✓		✓	✓	✓	✓								✓	
FIA_UAU.4/PACE	✓		✓	✓	✓	✓									
FIA_UAU.5/PACE	✓		✓	✓	✓	✓									
FIA_UAU.6/PACE				✓	✓	✓									

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**	**OT.PIN_PrK_Management**	**OT.Access_Control_Sign_Objects**	**OT.Signature_Generation**
FIA_UAU.6/EAC	✓		✓	✓	✓	✓									
FIA_API.1		✓													
FDP_ACC.1/TRM	✓		✓	✓		✓									
FDP_ACC.1/PIN	✓		✓	✓		✓								✓	
FDP_ACF.1/TRM	✓		✓	✓		✓									
FDP_ACF.1/PIN	✓		✓	✓		✓								✓	
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			✓	✓	✓	✓									

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	OT.PIN_PrK_Management	OT.Access_Control_Sign_Objects	OT.Signature_Generation
FMT_MTD.1/KEY_READ	✓	✓	✓	✓	✓	✓									
FMT_MTD.1/KEY_CHANG			✓												
FMT_MTD.1/PIN_Management													✓		
FMT_MTD.1/PrK_Management													✓		
FMT_MTD.3	✓														
FPT_EMS.1			✓						✓						
FPT_TST.1									✓			✓			
FPT_FLS.1									✓			✓			
FPT_PHP.3									✓		✓				
FTP_ITC.1/PACE				✓	✓	✓				✓					

6.6 SECURITY ASSURANCE REQUIREMENTS RATIONALE

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

7 TOE SUMMARY SPECIFICATION

7.1 SECURITY FEATURES

Security Features of the AKIS GEZGIN_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.

7.1.1 SF_PP: PHYSICAL PROTECTION

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

7.1.2 SF_DPM: DEVICE PHASE MANAGEMENT

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

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

7.1.3 SF_AC: ACCESS CONTROL AND SECURITY MANAGEMENT

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, and Signatory.

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

The TOE restricts to write the 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 create eMRTD / IDL application,
- 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 MRD after successful authentication,
- to create a template of e-Signature application.

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 MRD.

Users of the role **Signatory** are allowed to perform change and unblock PINs and e-Signature generation operations once they authenticate themselves by verifying PINs associated with the asymmetric private keys to be used.

The **Extended Inspection System** is the only role with Read access to Fingerprint and Iris data of the logical MRD. 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 [161] of the logical MRD,
- to read any of the EF.DG1 to EF.DG16 [162] of the logical MRD 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

[161] For IDL: EF.DG14

[162] For IDL: EF.DG14

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, the SFRs covered by SF_AC are FIA_AFL.1/PIN, FDP_ACC.1/TRM, FDP_ACC.1/PIN, FDP_ACF.1/TRM, FDP_ACF.1/PIN, FDP_UCT.1/TRM, FDP_UIT.1/TRM, 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/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/PA, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_CHANG, FMT_MTD.1/KEY_READ, FMT_MTD.1/PIN_Management, FMT_MTD.1/PrK_Management, FMT_MTD.3, and FTP_ITC.1/PACE.

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

7.1.4 SF_SM: SECURE MESSAGING

The TOE has SF_SM which allows the TOE to communicate to the external world securely. Secure Messaging feature protects the confidentiality, 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 SAC / Chip Authentication).

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 an 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, and FDP_RIP.1.

7.1.5 SF_IA: IDENTIFICATION AND AUTHENTICATION

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

- Manufacturer and Personalization Agent authentication,
- PACEv2 protocol,
- Chip authentication mechanism of EAC,
- Terminal authentication mechanism of EAC,
- PIN verification

The eMRD Manufacturer and the Personalization Agent authenticates themselves to the eMRD 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 Inspection System and the eMRD mutually authenticate each other by means of a PACEv2 protocol.

The eMRD and the Inspection System perform a Diffie-Hellman (DH or ECDH) key agreement by means of keys derived from Document Number/MRZ or CAN or SAI. 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 eMRD inspection is performed on a General Inspection System or an Extended Inspection System, then the MRD'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 ISO 11770-3 [16]. Chip Authentication proves that the chip is genuine and also provides strong keys for Secure Messaging.

If eMRD inspection is performed on an Extended Inspection System, then after a successful Chip Authentication the MRD'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.

For e-Signature generation operations, users can authenticate themselves by selecting and verifying PINs that are associated with asymmetric private keys to be used. If "non-repudiation" attribute is set for an asymmetric private key object, the user must verify the associated PIN before each e-Signature generation operation.

Therefore, the SFRs FCS_COP.1/AUTH, FCS_COP.1/SIG_VER, FCS_RND.1, 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, FIA_AFL.1/PIN, and FIA_API.1 are covered.

7.1.6 SF_CSUP: CRYPTOGRAPHIC SUPPORT

The hardware provides many cryptographic operations as detailed in the platform IC ST to which the composite TOE defined in this ST adds the cryptographic operation of signature generation.

Covered SFR is FCS_COP.1/SIG_GEN.

7.2 SECURITY FUNCTIONS RATIONALE

Table 20 shows the assignment of security functional requirements to TOE's security functionality.

Table 20: Coverage of SFRs by TOE Security Features

Security Functional Requirement	**SF_PP**	**SF_DPM**	**SF_AC**	**SF_SM**	**SF_IA**	**SF_CSUP**
FAU_SAS.1		✓	✓			
FCS_CKM.1/DH_PACE				✓		
FCS_CKM.1/CA				✓		
FCS_CKM.4				✓		
FCS_COP.1/AUTH					✓	

Security Functional Requirement	SF_PP	SF_DPM	SF_AC	SF_SM	SF_IA	SF_CSUP
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_COP.1/SIG_GEN						✓
FCS_RND.1					✓	
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					✓	
FIA_AFL.1/PIN			✓		✓	
FIA_API.1					✓	
FDP_ACC.1/TRM			✓			
FDP_ACC.1/PIN			✓			
FDP_ACF.1/TRM			✓			
FDP_ACF.1/PIN			✓			
FDP_UCT.1/TRM			✓			
FDP_UIT.1/TRM			✓			
FDP_RIP.1				✓		
FMT_SMF.1			✓			
FMT_SMR.1/PACE			✓			
FMT_LIM.1		✓	✓			
FMT_LIM.2		✓	✓			
FMT_MTD.1/INI_ENA			✓			

Security Functional Requirement	**SF_PP**	**SF_DPM**	**SF_AC**	**SF_SM**	**SF_IA**	**SF_CSUP**
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_CHANG			✓			
FMT_MTD.1/KEY_READ			✓			
FMT_MTD.1/PIN_Management			✓			
FMT_MTD.1/PrK_Management			✓			
FMT_MTD.3			✓			
FTP_ITC.1/PACE			✓			
FPT_EMS.1	✓					
FPT_FLS.1	✓					
FPT_PHP.3	✓					
FPT_TST.1	✓					

8 STATEMENT OF COMPATIBILITY

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

8.1 PP CONFORMANCE RATIONALE

Contents of this section was removed in Security Target Lite.

8.2 PLATFORM CONFORMANCE RATIONALE

Contents of this section was removed in Security Target Lite.

8.3 COMPATIBILITY: SECURITY REQUIREMENTS

8.3.1 SECURITY FUNCTIONAL REQUIREMENTS

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

Table 21: Platform SFRs - Compatibility Statement

No	Platform SFR	Category[163]	Related TSF
1.	FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3
2.	FRU_FLT.2	RP_SFR-MECH	FPT_TST.1
3.	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1
4.	FDP_IFC.1	RP_SFR-MECH	FPT_EMS.1
5.	FPT_TST.1	RP_SFR-MECH	Covered by ADV_IMP.1
6.	FDP_ITT.1	RP_SFR-MECH	FPT_EMS.1

[163] Either “IP_SFR”: irrelevant, “RP_SFR-SERV”: relevant in TSFI implementation or “RP_SFR-MECH”: relevant and addressed in ARC

7.	FPT_ITT.1	RP_SFR-MECH	FPT_EMS.1
8.	FMT_LIM.1	RP_SFR-MECH	FMT_LIM.1
9.	FMT_LIM.1/Loader	RP_SFR-MECH	Covered by ADV_IMP.1
10.	FMT_LIM.2	RP_SFR-MECH	FMT_LIM.2
11.	FMT_LIM.2/Loader	RP_SFR-MECH	Covered by ADV_IMP.1
12.	FCS_RNG.1/PTG.2	IP_SFR	
13.	FCS_RNG.1/DRG.4	RP_SFR-SERV	FCS_RND.1
14.	FCS_RNG.1/PTG.3	IP_SFR	
15.	FCS_COP.1/TDES	IP_SFR	
16.	FCS_COP.1/TDES_LIB	RP_SFR-SERV	FCS_COP.1/PACE_ENC FCS_COP.1/CA_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC
17.	FCS_COP.1/AES	IP_SFR	
18.	FCS_COP.1/AES_LIB	RP_SFR-SERV	FCS_COP.1/AUTH FCS_COP.1/PACE_ENC FCS_COP.1/CA_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC
19.	FCS_CKM.4/TDES	IP_SFR	
20.	FCS_CKM.4/TDES_LIB	RP_SFR-MECH	Covered by ADV_IMP.1
21.	FCS_CKM.4/AES	IP_SFR	

22.	FCS_CKM.4/AES_LIB	RP_SFR-MECH	Covered by ADV_IMP.1
23.	FAU_SAS.1	RP_SFR-MECH	FAU_SAS.1
24.	FDP_ACC.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
25.	FDP_ACF.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
26.	FDP_UCT.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
27.	FDP_UIT.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
28.	FDP_SDC.1	RP_SFR-MECH	FPT_PHP.3
29.	FDP_SDI.2	RP_SFR-MECH	FPT_PHP.3
30.	FTP_ITC.1/Loader	RP_SFR-MECH	Covered by ADV_COMP.1 and AGD_OPE.1
31.	FCS_COP.1/RSA	RP_SFR-SERV	FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/SIG_VER FCS_COP.1/SIG_GEN
32.	FCS_CKM.5/RSA_PubKeyDerivation	RP_SFR-SERV	FCS_COP.1/SIG_GEN
33.	FCS_CKM.1/RSA_KeyGen	IP_SFR	
34.	FCS_CKM.4/RSA	RP_SFR-MECH	Covered by ADV_IMP.1
35.	FCS_COP.1/ECDSA	RP_SFR-SERV	FCS_COP.1/SIG_VER FCS_COP.1/SIG_GEN

36.	FCS_COP.1/ECC_DHKE	RP_SFR-SERV	FCS_CKM.1/DH_PACE FCS_CKM.1/CA
37.	FCS_CKM.1/ECC_KeyGen	IP_SFR	
38.	FCS_CKM.4/ECC	RP_SFR-MECH	Covered by ADV_IMP.1
39.	FCS_COP.1/SHA	RP_SFR-SERV	FCS_CKM.1/DH_PACE FCS_CKM.1/CA FCS_COP.1/SIG_VER FCS_COP.1/SIG_GEN
40.	FMT_SMF.1	RP_SFR-MECH	FPT_FLS.1 FPT_PHP.3
41.	FDP_ACC.1/ACP	RP_SFR-MECH	FPT_FLS.1
42.	FDP_ACF.1/ACP	RP_SFR-MECH	FPT_FLS.1
43.	FMT_MSA.1/ACP	RP_SFR-MECH	FPT_EMS.1 FPT_FLS.1 FPT_PHP.3
44.	FMT_MSA.3/ACP	RP_SFR-MECH	FPT_EMS.1 FPT_FLS.1 FPT_PHP.3
45.	FCS_COP.1/AES_PUF	IP_SFR	
46.	FCS_COP.1/MAC_PUF	IP_SFR	
47.	FCS_CKM.1/PUF	IP_SFR	
48.	FCS_CKM.4/PUF	IP_SFR	

8.3.2 SECURITY ASSURANCE REQUIREMENTS

The level of assurance of the TOE is EAL 5 augmented with AVA_VAN.5 and ALC_DVS.2.

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

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

9 ABBREVIATIONS AND DEFINITIONS

3DES: Triple DES

AA: Active Authentication

AES: Advanced Encryption Standard

APDU: Application Packet Data Unit

BAC: Basic Access Control

BAP: Basic Access Protection

BIS: Basic Inspection System

BIS-PACE: Basic Inspection System with PACE

CA: Chip Authentication

CAN: Card Access Number

CPU: Central Processing Unit

CSCA: Country Signing Certification Authority

CVCA: Country Verifying Certification Authority

DES: Data Encryption Standard

DF: Dedicated File

DFA: Differential Fault Analysis

DPA: Differential Power Analysis

EAC: Extended Access Control

EAL: Evaluation Assurance Level

ECC: Elliptic Curve Cryptography

EF: Elementary File

EIS: Extended Inspection System

ES: Embedded Operating System

GIS: General Inspection System

IC: Integrated Circuit

ICAO: International Civil Aviation Organization

IDL: ISO-compliant Driving License

MF: Master File

MRD: Machine Readable Document

MRTD: Machine Readable Travel Document

MRZ: Machine Readable Zone

N/A: Not Applicable

NVM: Non-Volatile Memory

OSP: Organizational Security Policy

PA: Passive Authentication

PACE: Password Authenticated Connection Establishment

PP: Protection Profile

RAM: Random Access Memory

RSA: Ron Rivest, Adi Shamir and Leonard Adleman

ROM: Read Only Memory

SAC: Supplemental Access Control

SAI: Scanning Area Identifier

SAR: Security Assurance Requirements

SHA: Secure Hash Algorithm

SPA: Simple Power Analysis

SFR: Security Functional Requirement

ST: Security Target

TA: Terminal Authentication

TOE: Target of Evaluation

TPDU: Transmission Protocol Data Unit

10 REFERENCES

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

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

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

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

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

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

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

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

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

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

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

[12] 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 March 2012

[13] Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.10, 20 March 2012

[14] Technical Guideline TR-03111 Elliptic Curve Cryptography, Version 2.0, 2012-06-28

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

[16] ISO/IEC 11770-3:2021 Information security – Key management – Part 3: Mechanisms using asymmetric techniques, Fourth edition, 2021-10

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

[18] PKCS#1: RSA Cryptography Specifications, Version 2.2, RSA Laboratories, November 2016

[19] PKCS #15: Cryptographic Token Information Syntax Standard, Version 1.1, RSA Laboratories, June 6, 2016

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

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

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

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

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

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

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

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

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

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

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

[31] BSI TR-02101-2 BSI Technical Guideline – Cryptographic Mechanisms: Recommendations and Key Lengths, 2022-01

[32] SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, SOG-IS Crypto Working Group, version 1.2, January 2020