ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration

Security Target Lite

Rev. 3.9 — 13 July 2022
Release

PUBLIC

Document information

Info	Content
Keywords	Common Criteria, Security Target Lite, ChipDoc v3.1, JCOP 4 P71, ICAO EAC(1&2), PACE
Abstract	Security Target Lite of ChipDoc v3.1 application on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration, which is developed and provided by NXP Semiconductors, Business Unit Identification according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at Evaluation Assurance Level 5 augmented.

Revision history

Rev	Date	Description
1.0	2020-10-29	Initial Version of this Security Target Lite
3.5	2020-12-04	Updated STLite title, updated platform reference, aligned STLite versioning with ST
3.6	2020-12-18	Corrected a typo, updated platform reference, updated ICAO personalization guide reference
3.7	2021-02-26	Updated IC and Platform references
3.8	2022-06-21	Update of hardware IC and JavaCard Platform references. Update of FCS_CKM.1/DH_PACE SFR. Added new guidance document ChipDoc V3 Application Note.
3.9	2022-07-13	Update JCOP 4 P71 ST version

Contact information

For more information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. ST Introduction (ASE_INT)

1.1 ST Reference and TOE Reference

Table 1. ST Reference and TOE Reference

ST Title	ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration Security Target Lite
ST Reference	CDv3.1_2_31339_STLite_CDv3.1_ICAO_EAC_PACE
ST Version	Revision 3.9
ST Date	2022-07-13
Product Type	Java Card Applet
TOE Name	ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration Version 3.1.6.52
CC Version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 5, April 2017 (Part 1 [1], Part 2 [2] and Part 3 [3])

1.2 TOE Overview

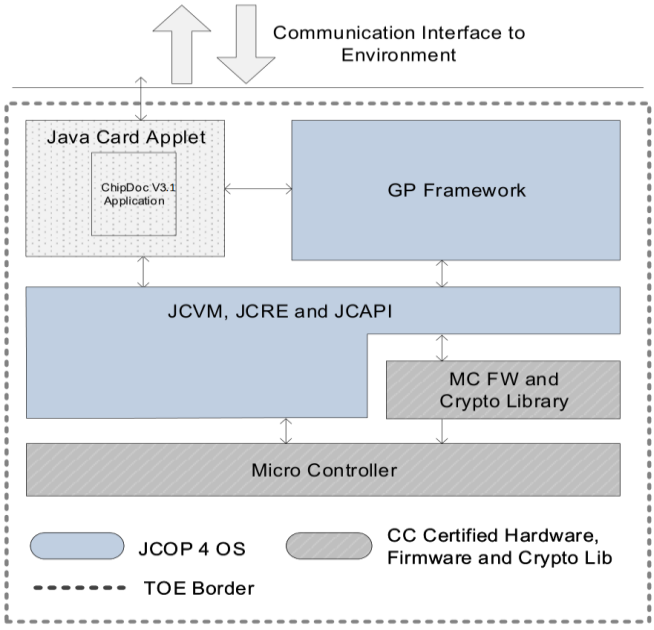


Fig 1. Components of the TOE

The TOE consists of an applet which is executed by a software stack that is stored on a Micro Controller. For a complete picture of the TOE see Figure 1, and for details with regards to the different components see section 1.3.1.

In ePassPort (ePP) configuration, the TOE is delivered in Closed Platform configuration, meaning that next to ChipDocv3.1 Applet, no other Applet can be installed. Inside the ChipDocv3.1 Applet, no other file system configuration can be installed beside the ePP system file.

In eDigitalIdentity (eDI) configuration, the TOE can be delivered in Open Platform configuration, meaning that next to ChipDocv3.1 Applet, other Applets can be installed. In that case the Platform Firewall enforces the domain separation between the different applets. Inside the ChipDocv3.1 Applet, other file system configurations can also be installed beside the eDI file system allowing several configurations (certified or not) to live on the same chip. In that case the file system enforces the domain separation between configurations.

The protection profiles [5] and [6] define the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). This ST extends this PP to contact, contactless and dual interface smartcard modules. It addresses the advanced security methods Basic Access Control (BAC), Standard Inspection Procedure (PACE), Extended Access Control version 1 and 2 (EAC1, EAC2),and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [11] and [12] for SAC (also known as PACE mechanism defined in [6]).

NB: in the current document, when EAC, CA, or TA are cited without further precision regarding version1 or 2, this means that both versions are concerned. When a distinction is needed, the version will be specified like EAC1, CA1, or TA1 (respectively 2).

ChipDoc v3.1 passport application is configurable in BAC or EAC with PACE chip authentication modes, with or without Active Authentication [11]. Also, it supports contact and contactless communication.

This ST applies to the EAC with PACE configuration with or without Active Authentication.

Note that there is no non-TOE hardware/software/firmware that is required by the TOE.

1.2.1 TOE Usage and Security Features for Operational Use

The ChipDoc v3.1 application offers variety of possible configurations like electronic identification (eID), electronic driver's license (eDL) or electronic passport (ePP), subject of the current TOE.

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this TOE contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip (such as CAN for PACE authentication) according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the

possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [11]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods (Passive Authentication) and the optional advanced security methods (BAC and/or SAC to the logical MRTD, Active Authentication of the MRTD's chip, EAC to the logical MRTD and the Data Encryption of additional sensitive biometrics) as optional security measure in the 'ICAO Doc 9303' [11]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

The BSI defines the additional mechanism EAC2 and PACE PIN in its TR03110-2 [13] to which Annex to PP0056v2 [37] complies.

This TOE addresses the protection of the logical MRTD (i) in integrity by write only- once access control and by physical means, and (ii) in confidentiality by the EAC1/EAC2 Mechanisms. This TOE addresses the AA as an optional security mechanism.

1.3 TOE Description

1.3.1 General

The TOE is an MRTD IC where application software is loaded to FLASH, and the TOE can be assembled in a variety of form factors. The main form factor is the electronic passport, a paper book passport embedding a contactless module.

The followings are an informal and non-exhaustive list of example graphic representations of possible end products embedding the TOE:

- Contactless interface cards and modules
- Dual interface cards and modules
- Contact only cards and modules

The scope of this TOE is covered in section 1.2 above and detailed hereafter.

The TOE is linked to a MRTD reader via its HW and physical interfaces.

- The contactless type interface of the TOE smartcard is ISO/IEC 14443 compliant.
- The optional contact type interface of the TOE smartcard is ISO/IEC 7816 compliant.

- The optional interfaces of the TOE SOIC-8 are ISO 9141 compliant.
- The optional interfaces of the TOE QNF-44 are JEDEC compliant.

There are no other external interfaces of the TOE except the ones described above.

The antenna and the packaging, including their external interfaces, are out of the scope of this TOE.

The TOE may be applied to a contact reader or to a contactless reader, depending on the external interface type(s) available in its form factor. The readers are connected to a computer and allow application programs (APs) to use the TOE.

The TOE can embed other secure functionalities, but they are not in the scope of this TOE and subject to an evaluation in other TOEs.

1.3.2 MRTD's Chip

For this TOE the MRTD is viewed as unit of

1. The **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
   a. the biographical data on the biographical data page of the passport book,
   b. the printed data in the Machine Readable Zone (MRZ) and
   c. the printed portrait.
2. The **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [11] (completed by [34] for eDigitalIdentity) as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
   a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   b. the digitized portraits (EF.DG2),
   c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
   d. the other data according to LDS (EF.DG5 to EF.DG16, EF.COM, EF.CardAccess, EF.CardSecurity) and
   e. the Document security object stored in EF.SOD.

This TOE addresses the protection of the logical MRTD:

- in integrity by write-only-once access control and by physical means, and
- in confidentiality by the SAC and Extended Access Control Mechanism.

This TOE addresses the Chip Authentication described in [12] as an alternative to the Active Authentication stated in [11].

1.3.3 Basic Access Control

The confidentiality by Basic Access Control (BAC) is a mandatory security feature that is implemented by the TOE. For BAC, the inspection system

(i) reads optically the MRTD,

(ii) authenticates itself as an inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [11], normative appendix 5.

In compliance with the ICAO Extended protection profile [5], this ST requires the TOE to implement the Chip Authentication defined in [12]. The Chip Authentication prevents data traces described in [11], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps:

(i) the inspection system communicates by means of secure messaging established by Basic Access Control,

(ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,

(iii) the inspection system generates an ephemeral key pair,

(iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and

(v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

1.3.4 PACE

The confidentiality by Password Authenticated Access Control (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the "Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)" [6]. Note that [6] considers high attack potential.

For the PACE protocol according to [13], the following steps shall be performed:

(i) The travel document's chip encrypts a nonce with the shared password, derived from the MRZ, CAN, PIN or PUK data and transmits the encrypted nonce together with the domain parameters to the terminal

(ii) The terminal recovers the nonce using the shared password, by either (physically) reading the MRZ or CAN data, or processing PIN or PUK data provided by the document holder.

(iii) The travel document's chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

1.3.5 Extended Access Control 1

In compliance with the ICAO Extended protection profile [5], this ST requires the TOE to implement the Extended Access Control as defined in [12]. The Extended Access Control consists of two parts:

(i) the Chip Authentication Protocol and

(ii) the Terminal Authentication Protocol.

The Chip Authentication Protocol:

(i) authenticates the MRTD's chip to the inspection system and

(ii) establishes secure messaging which is used by Terminal Authentication to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

Therefore Terminal Authentication can only be performed if Chip Authentication has been successfully executed. The Terminal Authentication Protocol consists of

(i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and

(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificate.

1.3.6 Extended Access Control 2

Based on EAC2 protection profile [39], this ST requires the TOE to implement the Extended Access Control 2 as defined in [13]. The Extended Access Control 2 consists of two parts that are necessarily following a PACE agreement:

(i) the Terminal Authentication Protocol 2 and

(ii) the Chip Authentication Protocol 2.

The Terminal Authentication Protocol 2 consists of:

(i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and

(ii) an access control by the TOE to allow reading the sensitive data only to successfully authenticated authorized inspection systems.

The Chip Authentication protocol 2 is performed only if the Terminal Authentication 2 has been successfully executed. The Chip Authentication protocol 2 consists of:

(i) authenticates the MRTD's chip to the inspection system and

(ii) establishes secure messaging to protect the confidentiality and integrity of the sensitive data during their transmission from the TOE to the inspection system.

The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificate.

1.3.7 Active Authentication

This TOE offers an optional mechanism called Active Authentication and specified in [12] section 1.2. This security feature is a digital security feature that prevents cloning by introducing a chip-individual key pair:

(i) The public key is stored in data group DG15 and thus protected by Passive Authentication.

(ii) The corresponding private key is stored in secure memory and may only be used internally by the MRTD chip and cannot be read out.

Thus, the chip can prove knowledge of this private key in a challenge-response protocol, which is called Active Authentication. In this protocol the MRTD chip digitally signs a challenge randomly chosen by the inspection system. The inspection system recognizes that the MRTD chip is genuine if and only if the returned signature is correct. Active Authentication is a straightforward protocol and prevents cloning very effectively but introduces a privacy threat: Challenge Semantics (see Appendix F for a discussion on Challenge Semantics).

1.3.8 TOE Components and Composite Certification

The certification of this TOE is a composite certification. This means that for the certification of this TOE other certifications of components which are part of this TOE are re-used. In the following sections more detailed descriptions of the components of Figure 1 are provided. In the description it is also made clear whether a component is covered by a previous certification or whether it is covered in the certification of this TOE.

1.3.8.1 Micro Controller

The Micro Controller is a secure smart card controller from NXP's SmartMX3 family. The Micro Controller contains a co-processor for symmetric cryptographic operations, supporting DES and AES, as well as an accelerator for asymmetric cryptographic algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory.

Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

The Micro Controller has been certified in a previous certification and the results are re-used for this certification. The exact reference to the previous certification is given in the following table:

Table 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library

Name	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3)
Certificate	BSI-DSZ-CC-1136-V2-2022
Reference	[28]

1.3.8.2 Security IC Dedicated Software

Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to volatile and non-volatile memory.

The Micro Controller Firmware has been certified together with the Micro Controller (refer to Table 2) and the same references [28] as given for the Micro Controller also apply for the Micro Controller Firmware.

Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The symmetric cryptographic operations comprise the algorithms 3DES, AES and KoreanSEED, where these algorithms use the symmetric co-processor of the Micro Controller. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

The Crypto Library has been certified together with the Micro Controller (refer to Table 2) and the same references [28] as given for the Micro Controller also apply.

1.3.8.3 Security IC Embedded Software

JCOP 4 P71

The Operating System consists of JCVM, JCRE, JCAPI and GP framework. It is implemented according to the Java Card Specification and GlobalPlatform and has been certified in the course of a previous certification, where the results are re-used for this certification. The exact reference to the certification is given in the following table:

Table 3. Reference to certified Platform

Name	JCOP 4 P71
Configurations relevant for this TOE	JCOP 4 P71 v4.7 R1.00.4 JCOP 4 P71 v4.7 R1.01.4
Certificate	NSCIB CC-22-180212
Reference	[29]

ChipDoc v3.1 application

The Target of Evaluation (TOE) is the integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [11] (completed by [34] for eDigitalIdentity) and providing the EAC1, EAC2 and SAC mechanisms according to the 'ICAO Doc 9303' [11] and BSI TR-03110-2 [13] ..

The TOE comprises at least:

- the circuitry of the MRTD's chip (N7121 IC)
- the IC Embedded Software (JCOP 4 P71 Operating System)
- the MRTD application (ChipDoc v3.1 applet in ePassPort/eDigitalIdentity configuration)
- the associated guidance documentation

TOE Configurations

The TOE is available in the following two configurations:

Table 4. ChipDoc v3.1 P71 configurations and identification

Configuration	ChipDoc v3.1 version	Identification
Configuration “Passport” (ePP)	3.1.6.52	Section 2.3.2 in [31]
Configuration “eDigitalIdentity” (eDI)	3.1.6.52	Section 2.3.3 in [31]

Both configurations offer the same functionality since provided by the same version of the Chipdoc v3.1 application, hence the configurations are distinguished only in terms of pre-personalization of the TOE. Both configurations are very close and rely on the same ICAO data structure and protocols with light differences. Consequently, they are both treated in the current security target. The distinction is motivated since different set of Security Functional Requirements are claimed for the two configurations in order to conform with the requirements specified in [37].

Note that in the remainder of the document, the terminology related to the two configurations might differ though expressing the similar content. An overview of the relevant terms is provided in the following table (c.f. related table in [37]):

Table 5. Terminology synonyms for the configurations

Configuration “Passport”	Configuration “eDigitalIdentity”
Travel document	eDigitalIdentity
Travel document holder	eDigitalIdentity document holder
Traveler	eDigitalIdentity document presenter
BIS-PACE	PACE terminal

It holds that terms related to configuration “passport” are generic terms and related statements apply for Configuration “eDigitalIdentity” as well, while terms related to configuration “eDigitalIdentity” are used to emphasize specific “eDigitalIdentity” context and according statements not necessarily can be propagated to the more generic “passport” context. This is due to the nature of “eDigitalIdentity” related requirements partially being more restrictive than in the more generic “passport” context (see also section 0)

1.3.9 TOE Lifecycle

The TOE lifecycle is shown hereafter and is described in terms of the four life cycle phases (subdivided to 7 steps) mentioned in PP0055 [3], but with a refinement in pre-personalisation, to support platform patching by the MRTD manufacturer who operates from a CC certified site.

The IC Developer, IC Manufacturer as well as the MRTD Embedded Software Developer of this TOE is NXP Semiconductors. In particular the software development for this composite TOE mainly took place at “NXP Gratkorn, Mikron-Weg 1, A-8101 Gratkorn, Austria” and “NXP Glasgow, Pegasus House, Scottish Enterprise Technology Park, Bramah Ave, East Kilbride Glasgow, G75 ORD, Scotland United Kingdom. All other sites contributing to the Lifecycle of this TOE can be read from the ALC_LCD evidence. .

1.3.9.1 Phase 1 “Development”

(Step 1 – IC Design)

The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step 2 – Embedded Software Design)

The embedded 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 operating system, the MRTD application and the guidance documentation associated with these TOE components.

1.3.9.2 Phase 2 "Manufacturing"

(Step 3 – IC Manufacturing)

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

(Step 4 – IC Initialisation)

The Embedded Software which constitutes the Operating System and the Card Content Manager is enabled with the requisite keys loaded and transport mechanisms enabled, which supports the secure transport of the IC from NXP manufacturing facility to the MRTD Manufacturer facility.

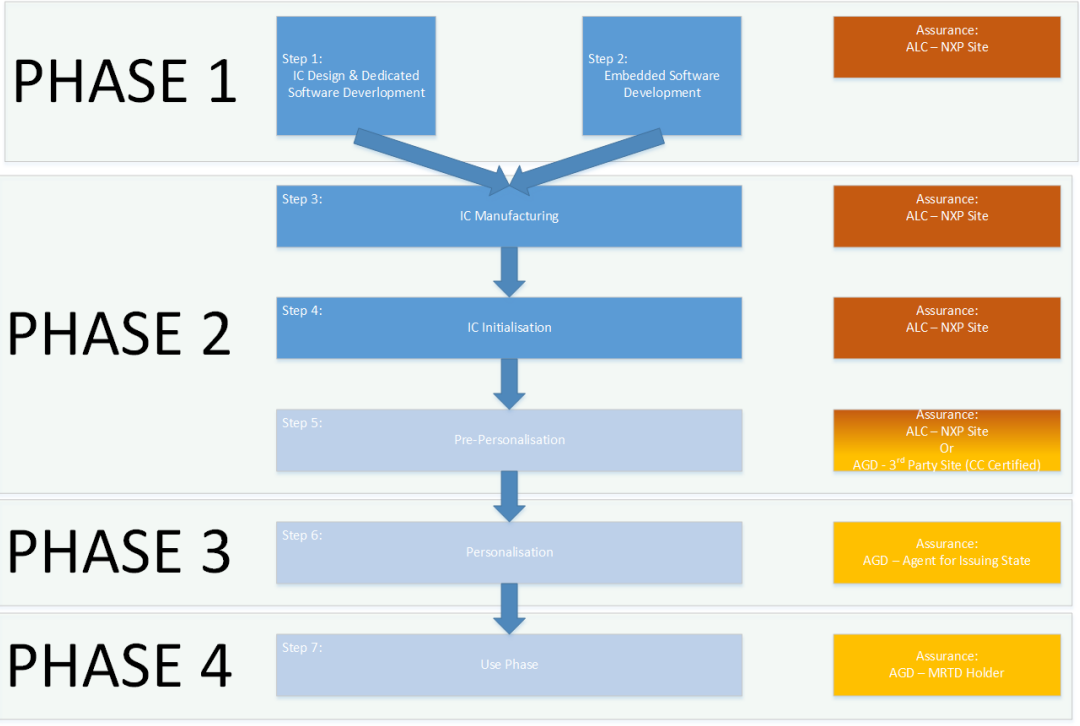


Fig 2. TOE Life Cycle

(Step 5 - PrePersonalisation)

During the step Pre-Perso, the MRTD manufacturer

(i) creates the MRTD application and

(ii) equips MRTD's chips with pre-personalization Data.

IC Pre-Personalization

To create the application, it is necessary to instantiate the applet and create ePP and/or eDI MRTD file systems. In addition to the certified MRTD file systems, one or more additional file systems may be present on the TOE. This allows the TOE user to switch between several (potentially certified) file systems or configurations of the application. Since the ChipDoc v3.1 application offers electronic identity, driving license or SSCD functionalities in addition to ePP and eDI, the associated file systems may coexist on the TOE.

Any platform patching required is completed at this point. For ePP/eDI products, Card Content Management is finalized in this phase, thus post issuance applet loading is disabled and the platform closed to further amendments.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. NXP or the MRTD Manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

(Packaging)

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

IC Packaging

MRTD Manufacturing

This step corresponds to the integration of the hardware and firmware components into the final product body. The TOE is protected during transfer between various parties. IC Packaging and MRTD Manufacturing are not part of the scope of this TOE.

1.3.9.3 Phase 3 "Personalization of the MRTD"

(Step 6 - Personalization)

The personalization of the MRTD includes:

- the survey of the MRTD holder's biographical data,
- the enrolment of the MRTD holder biometric reference data,
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD and
- configuration of the TSF if necessary.

The step 6 is performed by the Personalization Agent and includes but is not limited to the creation of the digital MRZ data (EF.DG1), the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both, the other data according to LDS (EF.DG5 to EF.DG16) and the Document security object. The signing of the Document security object by the Document signer [11] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD

(together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Personalization – 3rd Party Personalization facility

The TOE is protected during transfer between various parties by the confidential information which resides in the card during mask production.

In case the personalization is done by 3rd party personalization facility, the Personalization phase is not part of the scope of this TOE.

1.3.9.4 Phase 4 “Operational Use”

Where upon the card is delivered to the MRTD holder and until MRTD is expired or destroyed.

(Step 7)

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

The Operational Use phase is not part of the scope of this TOE.

1.3.10 TOE Identification

1.3.10.1 TOE Delivery

The TOE delivery can occur at the end of Step4 or at the end of Step5 (see chapter 1.3.9). The delivery comprises the following items:

Table 6. Delivery Items

Type	Name	Version	Form of delivery
JCOP 4 P71 Platform	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library ROM Code (Platform ID) FLASH content (FLASH ID) Patch Code (Patch ID)	R1.00.4 R1.01.4	Micro Controller including on-chip software: Firmware, Crypto Library and JCOP 4 Operating System
ChipDoc v3.1 application	FLASH content	3.1.6.52	Application software loaded onto the IC
Document	ChipDoc 3.1 User Guide Manual [30]	3.0	Electronic Document
Document	ChipDoc 3.1 ICAO Personalization Guide [31]	3.3	Electronic Document
Document	ChipDoc 3.1 Crypto Guide [32]	1.0	Electronic Document
Document	ChipDoc V3 Application Note [33]	1.4	Electronic Document

1.3.10.2 Identification of the TOE

The TOE can be identified by

- identifying the JCOP 4 P71 platform: The IDENTIFY command shall be sent to the TOE to verify the correct values of Platform ID, the FLASH ID and the Patch ID as stated in section "2.2 Platform identification" of the Personalization Guidance for this TOE [31].

- identifying the ICAO application: The ChipDoc v3.1 application and the specific TOE configuration (ICAO EAC) can be verified according the respective instructions in section “2. Identification” of the Personalization Guidance for this TOE [31].
- Identifying the TOE configuration: according to Table 4.

1.3.11 Evaluated Package Types

A number of package types are supported for this TOE. All package types, which are covered by the certification of the used platform (see [29]), are also allowed to be used in combination with each product of this TOE.

The package types do not influence the security functionality of the TOE. They only define which pads are connected in the package and for what purpose and in which environment the chip can be used. Note that the security of the TOE is not dependent on which pad is connected or not - the connections just define how the product can be used. If the TOE is delivered as wafer the customer can choose the connection on his own.

2. Conformance Claims

2.1 CC Conformance Claim

The ST claims compliance with the following references:

- Common Criteria Version 3.1 Part 1 [1]
- Common Criteria Version 3.1 Part 2 [2] extended
- Common Criteria Version 3.1 Part 3 [3] conformant

Extensions are based on the Protection Profiles (PP [5] and PP [6]) presented in the next section:

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FIA_API.1 ‘Authentication Proof of Identity’
- FMT_LIM.1 ‘Limited capabilities’
- FMT_LIM.2 ‘Limited availability’
- FPT_EMSEC.1 ‘TOE emanation’

2.2 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented. The augmentations to EAL5 are:

- ALC_DVS.2, and
- AVA_VAN.5

2.3 PP Claim

This ST claims strict conformance to the following Protection Profiles:

Protection Profile [5] **Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP)**	
Version	1.3.2
Date	05th December 2012
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0056V2
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0056-V2-2012-MA-02
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Protection Profile [6] **Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)**	
Version	1.01
Date	22nd July 2014
Prepared by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Identification	PP0068V2
Approved by	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Registration	BSI-CC-PP-0068-V2-2011-MA-01
Assurance Level	Common Criteria 3.1 EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

Note : The PACE PIN and the EAC2 mechanisms are presented in this security target as additional packages to the protection profiles [5] and [6] claimed above. Nevertheless, those additional packages are heavily inspired by protection profiles BSI-CC-PP-0086 [39].Regarding [37], the ST is conformant to the core document, but partially conformant to the end Note regarding Security Service correction deployment.

The ICAO SAC and EAC PPs define the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods SAC and Extended Access Control and Chip Authentication similar to the Active Authentication in the Technical reports of 'ICAO Doc 9303' [11] along with its supplements [13] and [16].

This MRTD's IC does not limit the TOE interfaces to contactless: both contact and contactless interfaces are part of this TOE and the PPs content has been enhanced for this purpose.

Additions to the claims from the PPs [5] [6] have been added to the related sections of this Security Target and are listed including rationales in section 8.4 of this Security Target.

3. Security Problem Definition

3.1 Assets

3.1.1 ICAO assets

The assets to be protected by the TOE include the User Data on the travel document's chip, user data transferred between the TOE and the terminal, and travel document tracing data.

Logical travel document sensitive User Data

Sensitive biometric reference data (Integrity and Confidentiality):

- **EF.DG3**: Biometric Finger(s)
- **EF.DG4**: Biometric Eye(s) Iris

Logical MRTD data

The 'ICAO Doc 9303' [11] requires that Basic Inspection Systems must have access to the following logical data which integrity should always be preserved (integrity, Confidentiality and Authenticity when PACE is used):

- **EF.COM**: Common Data Elements, lists the existing EF with the user data
- **EF.SOD**: Document Security Object according to LDS [11] used by the inspection system for Passive Authentication of the logical MRTD
- **EF.CardAccess**: Security Information required for PACE
- **EF.CardSecurity:** Security Information required for PACE
- **EF.DG1**: document's data (Type, Issuing State or Organization, Number, Expiry Date, Optional Data), holder's data (Name, Nationality, Date of Birth, Sex) and Check Digits
- **EF.DG2**: Encoded Face (Global Interchange Feature)
- **EF.DG5**: Biometric Face
- **EF.DG7**: Displayed Signature or Usual Mark
- **EF.DG8**: Displayed Portrait
- **EF.DG9**: Data Feature(s)
- **EF.DG10**: Structure Feature(s)
- **EF.DG11**: Additional Personal Detail(s)
- **EF.DG12**: Additional Document Detail(s)
- **EF.DG13**: optional Detail(s)
- **EF.DG14**: Security Info (Chip Authentication Public Key Info)
- **EF.DG15**: Active Authentication Public Key Info
- **EF.DG16**: Person(s) to Notify

Due to interoperability reasons with 'ICAO Doc 9303' [11], the TOE specifies the BAC mechanisms with resistance against enhanced basic attack potential granting access to:

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16) (DG6 is absent),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

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

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD. This authenticity relies on the confidentiality and integrity of data such as the Active Authentication Public Key, PACE key, EF.CardAcces, EF.CardSecurity info or the Chip Authentication Private Key.

Additional assets from the PACE PP

The primary assets

- User data stored on the TOE,
- User data transferred between the TOE and the terminal connected, and
- Travel document tracing data,

And the secondary assets

- Accessibility to the TOE functions and data only for authorized subjects,
- Genuineness of the TOE,
- TOE internal secret cryptographic keys,
- TOE internal non-secret cryptographic material, and
- Travel document communication establishment authorization data.

3.1.2 Refinements relevant for configuration "eDigitialIdentity"

3.1.2.1 Primary Assets

***Application note**: The access to logical eDigitalIdentity document data contains in the DGx (defined in specification [38]) is allowed only after PACE PIN authentication*

***Application note**: eDigitalIdentity documentation communication establishment authorization data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorization attempt. The TOE shall secure the reference information as well as – together with the terminal connected – the*

verification information in the 'TOE<->terminal' channel, if it has to be transferred to the TOE. Please note that PACE PIN are not to be send to the TOE.

Sensitive Identification User Data

Person identification data, which have been classified as sensitive data by the eDigitalIdentity document issuer.

Sensitive identification user data are a subset of all user data.

Generic security property to be maintained by the current security policy: Confidentiality, Integrity, Authenticity.

***Application note**: Since sensitive identification user data are a subset of all user data, all threats and objectives applied to user data from [5] are also applied to sensitive identification use data.*

3.1.2.2 Secondary Assets

The secondary assets represent TSF and TSF-data in the sense of Common Criteria

eDigitalIdentity document Communication Establishment Authorization Data

Restricted- revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE PIN & PUK). These data are stored in the TOE and are not send to it.

Generic security property to be maintained by the current security policy: Confidentiality, Integrity.

Secret eDigitalIdentity document Holder Authentication Data

Secret authentication information for the eDigitalIdentity document holder being used for verification of the authentication attempts as authorized eDigitalIdentity document holder (sent PACE passwords, e.g. PIN or PUK).

Generic security property to be maintained by the current security policy: Confidentiality, Integrity.

3.2 Subjects

This Security Target considers the following subjects:

S.Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

S.Personalizer *Personalization Agent*

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [11].

S.Country_Sign *Country Signing Certification Authority*

An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see ICAO9303 [11].

S.Country *Country Verifying Certification Authority*

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

S.DS *Document Signer*

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object (SOD) that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificates, see ICAO9303 [11]. Note that this role is usually delegated to a Personalization Agent.

S.DV *Document Verifier*

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.

S.Terminal

A terminal is any technical system communicating with the TOE through the contactless or contact-based interface. The role terminal is the default role for any terminal being recognized by the TOE that is neither a PACE terminal nor an EAC1 nor an EAC2 terminal.

S.PACE Terminal

A technical system verifying correspondence between the password stored in the electronic document and the related value presented to the terminal by the electronic document presenter. A PACE terminal implements the terminal part of the PACE protocol and authenticates itself to the electronic document using a shared password

(CAN, PIN, PUK or MRZ). A PACE terminal is not allowed reading sensitive user data.

S.EAC1/2 Terminal

A terminal that has successfully passed Terminal Authentication 1 (respectively 2) is an EAC1 (respectively 2) terminal. Both are authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

S.IS-PACE *Inspection system*

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The **Basic Inspection System** (BIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The IS-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) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

S.Holder *MRTD Holder*

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

S.Traveler

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

3.2.1 Refinements relevant for configuration "eDigitialIdentity"

The following subject refines the subject S.BIS-PACE (Basic Inspection System PACE) as defined in [6], only relevant for configuration "eDigitalIdentity"

S.PACE-Terminal *PACE Terminal*

A technical system verifying correspondence between the password stored in the eDigitalIdentity document and the related value presented to the terminal by the eDigitialIdentity document present.

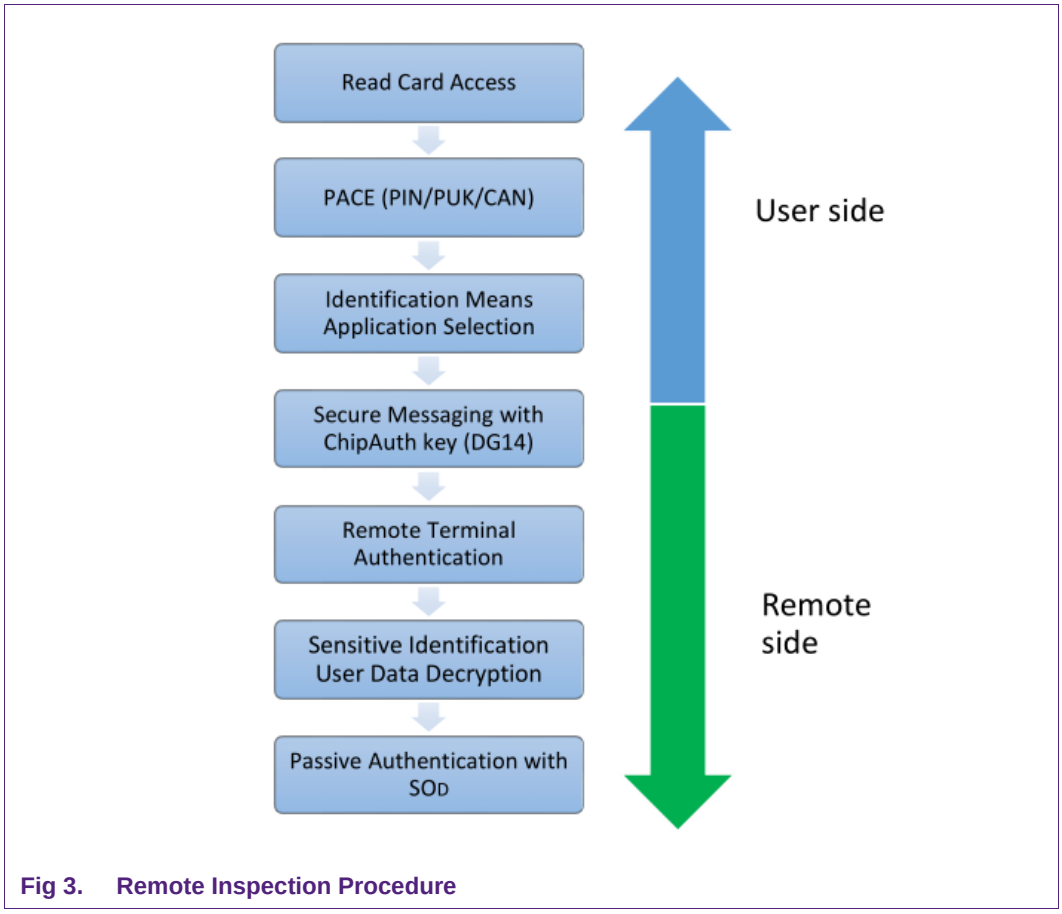


Fig 3. Remote Inspection Procedure

S.PACE-Terminal performs the Remote Inspection Procedure (see Fig 3) and therefore (i) contains a terminal for the communication with the eDigitalIdentity document's chip, (ii) implements the terminal part of the PACE protocol, (iii) authenticates the eDigitalIdentity holder to the eDigitalIdentity document using a shared password (PIN, PUK or CAN), and (iv) implements the Chip Authentication Protocols Version 1 according [13].

The remote terminal authentication, the decryption of sensitive identification user data and the passive authentication are performed outside the TOE.s

3.3 Assumptions

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

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 (with optional Active Authentication). BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure

access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

A.Passive_Auth *PKI for Passive Authentication*

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer

(i) generates the Document Signer Key Pair,

(ii) hands over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data.

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 are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

3.4 Threat agent

S.ATTACKER	A threat agent trying (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document. A threat agent trying to undermine the security policy defined by the current Security Target, especially to change the properties of the assets having to be maintained. This threat agent has high attack potential.

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

3.5 Threats

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Read_Sensitive_Data	*Read the sensitive biometric reference data*

An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.

The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [6]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

T.Sensitive_Data	*Untheorized access to sensitive user data*

An attacker tries to gain access to sensitive user data through the communication interface of the electronic document's chip.

The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack (sensitive data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

Threat agent having high attack potential, knowing the PACE password, being in possession of one or more legitimate electronic document. Asset: confidentiality of sensitive user data stored on the electronic document.

T.Counterfeit	*Counterfeit MRTD's chip*

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 to another appropriate chip to imitate this genuine travel document's chip.

T.Counterfeit/EAC2	*Counterfeit of electronic document chip data*

An attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part

of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for authentication of an electronic document presenter by possession of an electronic document.

The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document.

Threat agent having high attack potential, being in possession of one or more legitimate ID-Cards. Asset: authenticity of user data stored on the TOE.

T.Skimming *Skimming travel document / Capturing card-Terminal communication*

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/contact interface of the TOE.

T.Eavesdropping *Eavesdropping on the communication between the TOE and the PACE terminal*

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.

T.Tracing *Counterfeit MRTD's chip*

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/contact interface of the TOE.

T.Forgery *Forgery of data on MRTD's chip*

An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

T.Abuse-Func *Abuse of Functionality*

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 initialisation and personalisation in the operational phase after delivery to the travel document holder.

T.Information_Leakage *Information Leakage from MRTD's chip*

An attacker may exploit information leaking 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.

T.Phys-Tamper	*Physical Tampering*

An attacker may perform physical probing of the travel document in order

(i) to disclose the TSF-data, or

(ii) to disclose/reconstruct the TOE's 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 the TSF-data stored on the travel document.

T.Malfunction	*Counterfeit MRTD's chip*

An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to

(i) deactivate or modify security features or functionality of the TOE' hardware or to

(ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

3.5.1 Additional Threat relevant for configuration "eDigitialIdentity"

The following threat is only relevant for configuration "eDigitalIdentity":

T.Sensitive_ID_User_Data	*Unauthorized access to sensitive ID user data*

An attacker tries to gain access to sensitive identification user data through the communication interface of the eDigitalIdentity document's chip. The threat T.Sensitive_ID_User_Data is similar to the threat T.Skimming as defined in section 3.5 wrt the attack path (communication interface) and the motivation (to get data stored on the eDigitalIdentity document's chip) but differs from those in the asset under attack (sensitive identification use data vs. CAN, PIN, PUK and other data, the opportunity (i.e. knowing the PACE password) and therefore the possible attack methods.

3.6 Organisational Security Policies

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

P.Sensitive_Data	*Privacy of sensitive biometric reference data*

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document

Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

P.Manufact	*Manufacturing of the MRTD's chip*

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

P.Personalization	*Personalization of the MRTD by issuing State or Organization*

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

This PP includes all OSPs from the PACE PP, chap 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal. Due to identical definitions and names they are also not repeated here.

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 travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
3) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase.
4) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

P.Card_PKI	*PKI for Passive Authentication*

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 travel document Issuer shall publish the CSCA Certificate (CCSCA) .
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

(CCSCA) 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 (CDS) 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.

P.Terminal_PKI	*PKI for Terminal Authentication 2*

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

P.Trustworth_PKI	*Trustworthiness of the 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.

P.Terminal	*Abilities and trustworthiness of terminals*

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders.
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-Hellmann).
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 CCSCA and CDS) 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 PP.

P.EAC2_Terminal	*Abilities of terminals executing EAC Version2*

Terminals that intent to be EAC2 terminals must implement the respective terminal part of the protocols required to execute EAC version 2 according to [TR03110-2], and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

3.6.1 Additional OSP relevant for configuration “eDigitialIdentity”

The following OSP is only relevant for configuration “eDigitalIdentity”. It is introduced with the intention to cover the security service correction deployment as introduced in the last chapter of [33].

P.CASS_Replacement *Replacement of Chip Authentication Security Service*

The Security Service (i.e. cryptographic material including Private Key, Public Key in DG14, Signed HASH of Public Key in SOd, Key Size, Key Type) used for Chip Authentication can be replaced on request of an authorized user during the Usage phase of the eDigitalIdentity product (phase 7 of the TOE LifeCycle). There is no deployment of executable code post issuance. The replacement CASS(s) are prepared during the personalization phase of the TOE and only rely on natively supported algorithms. The replacement of the CASS is considered as a configuration operation of the TOE and can occur in the following environment:

- Administrative offices (secure environment)
- Professional environment (secure reader environment [Vital reader, ATM…])
- End-user Home (non-secure environment)

4. Security Objectives

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

Extensions to the security objectives from the PPs [5] [6] are underlined and listed in section 8.4.

4.1 SOs 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.Sens_Data_Conf	*Confidentiality of sensitive biometric reference data*

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) 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 must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Sens_Data_EAC2	*Confidentiality of sensitive user data*

The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE.

The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

OT.Chip_Auth_Proof	*Proof of MRTD's chip authenticity*

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

Application note: *The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD'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 MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [11] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

OT.CA2	*Proof of the Electronic Document's chip authenticity*

The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [TR03110-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.

OT.AA_Proof	*Proof of MRTD's chip authenticity by Active Authentication*

The TOE may support the Extended Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [11].

OT.Data_Int	*Integrity of data*

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity 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. Note: This Objective from PACE PP is extended to all kinds of PACE terminals and EAC2 terminals.

OT.Data_Aut	*Authenticity of data*

The TOE must 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 must 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) after the PACE Authentication. 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). Note: This Objective from PACE PP is extended to all kinds of PACE terminals and EAC2 terminals.

OT.Data_Conf	*Confidentiality of data*

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must 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 must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact 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 must 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 must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

OT.Prot_Phys-Tamper	*Protection against Physical Tampering*

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)
- with a prior
- reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction	*Protection against Malfunctions*

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

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

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

OT.AC_Pers	*Access Control for Personalization of logical MRTD*

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [11] and the TSF data can be written by authorized Personalisation 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 personalisation of the document.

Application note: *The OT.AC_Pers implies that:*

1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization,

2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.AC_Pers_EAC2	*Personalization of the Electronic Document*

The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2. This security objective for the TOE modifies OT.AC_Pers from PACE PP as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

OT.Identification	*Identification and Authentication of the TOE*

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

4.1.1 Additional SOs relevant for configuration “eDigitialIdentity”

The following security objectives are only relevant for configuration “eDigitalIdentity”:

OT.Sens_Ident_User_Data	*Confidentiality of sensitive identification user data*

The TOE must ensure the confidentiality of the sensitive identification user data by granting read access only to authorized inspection systems. The authorization of the inspection system is drawn by the eDigitialIdentity document holder by consciously entering his secret PIN. The sensitive identification user data may be decrypted to authorized inspection systems by the eDigitialIdentity document issuer State or Organisation. The TOE must ensure the confidentiality of the sensitive identification user data during their transmission to the inspection system. The confidentiality of the sensitive identification user data shall be protected against attacks with high attack potential.

Notice that the security objective OT.Chip_Auth_Proof as defined in section 4.1 is more clarified in the eDigitalidentity application by adding the following application note:

***Application note**: The OT.Chip_Auth_Proof implies the eDigitalIdentity document’s chip to have (i) a unique identity as given by the eDigitalIdentity document’s 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 eDigitalIdentity document’s chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the eDigitalIdentity document’s chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [38] and (ii) the hash value of DG14 in the Document Security Object singed by the Document Signer.*

OT.CASS_Replacement	*Replacement of Chip Authentication Security Service*

The TOE must ensure that the command used to replace CASS in the field can be sent only by an Authorized User.

The replacement of the CASS shall be performed in an Atomic way. All the operations needed for the new CASS to operate in the TOE shall be completed before its activation.

If the Atomic replacement is not successful (in case of interruption or incident), then the TOE shall remain in its initial state or fail secure.

***Application note**: This security objective is introduced with the intention to cover the security service correction deployment as described in [33]. Due to deployment process choice (no code upgrade in the field), this objective has been tailored to better match the real use case.*

- *As there is no field upgrade of the code, the identification data of the TOE remains unchanged and the requirement for its activation was removed from the objective.*
- *As the provisioning is performed during file system creation (pre-personalization phase) and the TSF installation data installation (personalization), the objective "O.Security_Service_Provisioning" specified in [33] was not retained (considered as no added value with regard to OT.AC_Pers). Nevertheless, the evidence of authenticity and integrity of the command for replacement of the CASS needs to be addressed in the current objective.*
- *As there is no field upgrade of the code, the objective "O.TOE_Identification" specified in [33] was not retained (no added value with regard to OT.Identification.*

4.2 Objective on the Environment

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

OE. Auth_Key_Travel_Document *Travel document authentication keys*

The issuing State or Organisation has to establish the necessary public key infrastructure in order to

(i) generate the travel document's Chip Authentication Key Pair,
(ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and
(iii) support inspection systems of receiving States or Organisations 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. Active_Auth_Key_Travel_Document *Travel document active authentication keys*

The issuing State or Organisation has to establish the necessary public key infrastructure in order to

(i) generate the travel document's Active Authentication Key Pair,
(ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15
(iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Active Authentication Public Key by means of the Document Security Object.

OE.Authoris_Sens_Data *Authorisation for Use of Sensitive Biometric Reference*

	Data

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

OE.Exam_travel_document	*Examination of the physical part of the travel document*

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller 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 Organisation, and (ii) implements the terminal part of PACE [4] and/or the Basic Access Control [11]. 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 Organisation 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_system	*Authorization of extended inspection system*

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.

OE.Legislative_Compliance	*Issuing of the travel document*

The travel document Issuer must issue the travel document 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 has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must

(i) generate a cryptographically secure CSCA Key Pair

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

(iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must

(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].

The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [11]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalization	*Personalization of logical MRTD*

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf

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

(ii) enrol the biometric reference data of the travel document holder,

(iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder,

(iv) write the document details data,

(v) write the initial TSF data,

(vi) sign the Document Security Object (in the role of a DS).

OE.Terminal	*Terminal Operating*

The terminal operators must operate their terminals as follows:

1) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [11].

2) The related terminals implement the terminal parts of the PACE protocol [3], of the Passive Authentication [3] (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-Hellmann).

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 CCSCA and CDS) 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]).

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 PP.

OE.Travel_Document_Holder	*Travel document holder obligations*

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

OE.Chip_Auth_Key	*Key Pairs needed for Chip Authentication*

The electronic document issuer has to ensure that the electronic document's chip authentication key pair is generated securely, that the private keys of these key pairs are stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110-2] to check the authenticity of the electronic document's chip. The TSF of PACE PP does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of PACE PP.

OE.Terminal_Authentication	*Key pairs needed for Terminal Authentication*

The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer. The TSF of PACE PP does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of the PACE password). Therefore, this additional security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of PACE PP.

4.2.1 Additional OEs relevant for configuration "eDigitialIdentity"

OE.CASS_Replacement	*Replacement of Chip Authenticate Security Service*

The Personalization agent must follow the ChipDoc3.1 ICAO Personalization Guide [31] and ChipDoc3.1 User Guidance Manual [30] to prepare the predefined Chip Authentication Security Services replacement material for eDigitalIdentity configuration only.

4.3 Security objectives rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

4.3.1 Security Objectives Coverage

The following table indicates that all security objectives of the TOE are traced back to threats and/or organizational security policies and that all security objectives of the environment are traced back to threats, organizational security policies and/or assumptions.

Note that T.Sensitive_ID_User_Data and OT_Sens_Ident_User_Data_Conf
P.CASS_Update are only relevant for configuration “eDigitalIdentity”

Threats Assumptions Policies / Security objectives	OT.Sens_Data_Conf	OT.Sens_Data_EAC2	OT.Chip_Aut_Proof	OT.CA2	OT.AA_Proof	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Sens_Ident_User_Data_Conf	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	**OT.CASS_Replacement**	OE.Auth_Key_Travel_Document	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Active_Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalisation	OE-Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance	OE.CASS_Replacement
T.Read_Sensitive_Data	X																						X			X						
T.Counterfeit			X		X														X			X		X								
T.Counterfeit/EAC2				X																X												
T.Skimming	X	X						X	X	X	X										X									X		
T.Eavesdropping	X	X								X	X																					
T.Sensitive_ID_User_Data											X																					
T.Sensitive_Data		X																			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	X			
P.Sensitive_data	X																						X			X						
P.Personalization						X									X												X					
P.Manufact															X																	
P.Pre-Operational						X	X								X												X				X	
P.Terminal																								X					X			
P.EAC2_Terminal																				X	X								X			
P.Terminal_PKI																					X											
P.Card_PKI																												X				
P.Thrustworthy_PKI																												X				
P.CASS_Replacement						X									X			X														X
A.Insp_Sys																								X	X							
A.Auth_PKI																							X			X						
A.Passive_Auth																								X				X				

Table 7. Security Environment to Security Objectives Mapping

4.3.2 Security Objectives Sufficiency

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/contact interface. This threat is countered by the security objectives **OT.Data_Inty**, **OT.Data_Aut**

and **OT.Data_Conf** through the PACE authentication. the threat is also addressed by **OT.Sens_Data** and **OT_Sens_Data_EAC2** that demands a trusted channel based on Chip Authentication 2, and requires that read access to sensitive user data is only granted to EAC terminals with corresponding access rights. Moreover, **OE.Terminal_Authentication** requires the electronic document issuer to provide the corresponding PKI. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal (PACE, EAC1, EAC2) in order to gain the User Data transferred there. This threat is countered by the security objective **OT.Data_Conf** through a trusted channel based on PACE Authentication, and by OT.Sens_Data and OT.Sens_Data_EAC2 demanding a trusted channel that is based on Chip Authentication 1 or 2.

The threat **T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless/contact 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).

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** and **OT_AC_Pers_EAC2** requires the TOE to limit the write access for the travel document to the trustworthy Personalisation Agent (cf. **OE.Personalisation**). 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_Int** and **OT.Data_Aut**, respectively. The objectives **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to **OE.Terminal** and performing the Passive Authentication using the Document Security Object as aimed by **OE.Passive_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally, the examination of the presented MRTD passport book 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 travel document.

The examination of the travel document 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” which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document’s chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** “Protection of data from the logical travel document” require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the 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.

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.

The threat **T.Counterfeit/EAC2** addresses the attack of an unauthorized copy or reproduction of the genuine electronic document. This attack is countered by the proof of the chip's authenticity, as aimed by OT.CA2 using a Chip Authentication key pair that is generated within the issuing PKI branch, as aimed by OE.Chip_Auth_Key. According to OE.Chip_Auth_Key, the terminal has to perform the Chip Authentication 2 protocol to verify the authenticity of the electronic document's chip.

The threat **T.Sensitive_Data** is countered by the TOE-Objective OT.Sens_Data_EAC2, that requires that read access to sensitive user data is only granted to EAC2 terminals with corresponding access rights. Furthermore, it is required that the confidentiality of the data is ensured during transmission. The objective OE.Terminal_Authentication requires the electronic document issuer to provide the public key infrastructure (PKI) to generate and distribute the card verifiable certificates needed by the electronic document to securely authenticate the EAC2 terminal.

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-personalisation Data as being fulfilled by **OT.Identification**.

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, OT_AC_Pers_EAC2** and **OE.Personalisation** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents'; **OE.Legislative_Compliance** is affine to the OSP's property 'compliance with laws and regulations'.

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.

The OSP **P.EAC2_Terminal** addresses the requirement for EAC2 terminals to implement the terminal parts of the protocols needed to executed EAC2 according to its specification in [TR03110-2], and to store (static keys) or generate (temporary keys and nonces) the needed related credentials. This is enforced by OE.Chip_Auth_Key which requires Chip Authentication keys to be correctly generated and stored, by OE.Terminal_Authentication for the PKI needed for Terminal Authentication, and by OE.Terminal which covers the PACE protocol and the Passive Authentication protocol.

The OSP **P.Terminal_PKI** is enforced by establishing the receiving PKI branch as aimed by the objective OE.Terminal_Authentication.

The OSP **P.Card_PKI** is enforced by establishing the issuing PKI branch as aimed by the objectives **OE.Passive_Auth_Sign** (for the Document Security Object).

The OSP **P.Trustworthy_PKI** is enforced by **OE.Passive_Auth_Sign** (for CSCA, issuing PKI branch).

The Assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly addressed by **OE.Passive_Auth_Sign** requiring the travel document 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 travel document.

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 Organisations only. The Document Verifier of the receiving State 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.

The OSP **P.Personalisation** “Personalisation of the travel document by issuing State or Organisation only” addresses the (i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** “Personalisation of logical 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 Personalisation of logical travel document”. Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation Agent.

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.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

The OSP P.Terminal “Abilities and trustworthiness of terminals” is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [6]. **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** “Counterfeit of travel document chip data” addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is

thwarted by chip identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** “Travel document Authentication Key”. According to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document’s chip.

In addition, the threat **T.Counterfeit** “Counterfeit of travel document chip data” is countered by chip identification and authenticity proof required by **OT.Active_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organisation. The Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** “Travel document Authentication Key”.

4.3.2.1 Additional Security Objectives Sufficiency relevant for configuration “eDigitalIdentity”

The following rationales are only relevant in the context of configuration “eDigitalIdentity”:

The threat **T.Skimming** addresses accessing the sensitive identification user data (stored on the TOE or transferred between the TOE and the terminal) using the TOE’s contactless/contact-based interface. Additionally to the security objectives from [5][6] which counter this threat, the threat is also addressed by **OT.Sens_Ident_User_Data_Conf** that demands a trusted channel based on Chip Authentication, and requires that read access to sensitive identification user data is only granted to authorized Inspection Systems.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a PACE terminal or an authorized Inspection Systems in order to gain access to transferred sensitive identification user data. Additionally to the security objective from [5][6] which counter this threat, the threat is also addressed by **OT.Sens_Ident_User_Data_Conf** that demands a trusted channel based on Chip Authentication.

The threat **T.Sentitive_ID_User_Data** is countered by the TOE-Objective **OT.Sens_Ident_User_Data_Conf** that requires that read access to sensitive identification user data is only granted to authorized Inspection Systems. Furthermore, it is required that the confidentiality of the data is ensured during transmission.

The OSP **P.CASS_Replacement** is enforced as follows: **OT.CASS_Replacement** ensures that the command used in the field to replace the CASS of a particular application is accessible to the authorized user (Issuer or any authorized user acting on behalf of Issuer) and that the replacement process is secured and atomic. There is no update of the code in the field. **OT.Sens_Data_Conf, OT.DATA_Int, OT.DATA_Auth and OT.DATA_Conf** ensure the protection of data exchange when CASS Replacement in invoked in user phase. **OT.AC_Pers** provides the needed functionality for CASS replacement preparation during the personalization phase. **OT.Identification** ensures that the TOE provides means to store and protect the original TOE identification data all along the product life. **OE.CASS_Replacement** will ensure that appropriate replacement

material is prepared during the personalization phase in order to be able to perform eDigitalIdentity CASS Replacement in the field. Those objectives together allow the Personalization Agent to securely load pre-created alternative CASS during the personalization phase of the document and allow the authorized user (typically the Personalization Agent) to securely invoke the CASS replacement in user phase.

5. Extended Components Definition

This ST contains the following extended components defined as extensions to CC part 2 in the claimed Protection Profile [5]:

- SFR FAU_SAS ‘Audit data storage’
- SFR FCS_RND ‘Generation of random numbers’
- SFR FIA_API ‘Authentication Proof of Identity’
- SFR FMT_LIM ‘Limited capabilities and availability’
- SFR FPT_EMSEC.1 ‘TOE emanation’

5.1 Audit data storage (FAU_SAS)

To define the security functional requirements of the TOE, a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements 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.

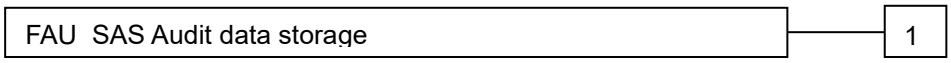
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling:



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	**The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.**

5.2 Generation of random numbers (FCS_RND)

To define the IT security functional requirements of the TOE, a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the 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.

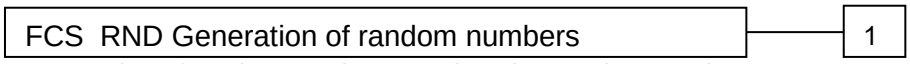
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	**The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].**

5.3 Authentication Proof of Identity (FIA_API)

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

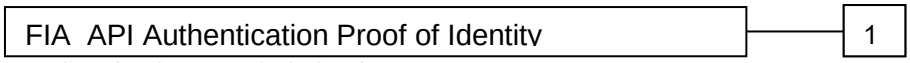
Application note: *The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria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

FIA_API Authentication Proof of Identity

Family behavior

This family defines functions provided by the TOE to prove their identity and to be verified by 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.
FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	**The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].**

5.4 Limited capabilities and availability (FMT_LIM)

The family FMT_LIM describes the functional requirements for the Test Features of the TOE.

The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

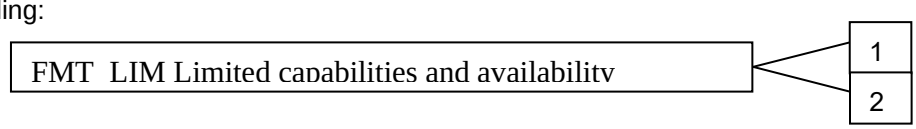
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts the access to functions whereas the 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 lifecycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. 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 show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 **The TSF shall be designed in a manner that limits their capabilities 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.

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*].**

Application note: *The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that:*

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

or conversely

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

The combination of both requirements shall enforce the policy.

5.5 TOE emanation (FPT_EMSEC.1)

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

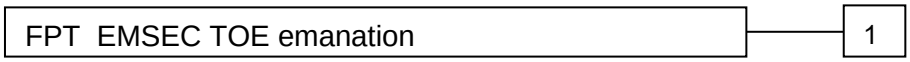
The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FPT_EMSEC TOE Emanation

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1	TOE Emanation has two constituents:
FPT_EMSEC.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMSEC.1.2	Interface Emanation requires not to emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	**The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].**
FPT_EMSEC.1.2	**The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].**

6. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Some security functional requirements represent extensions to [1].

Operations for assignment, selection and refinement have been made and are designated by an underline (e.g. none), in addition, where operations that were uncompleted in the PP [5] are also identified by *italic underlined* type.

The TOE security assurance requirements statement given in section 6.2 is drawn from the security assurance components from Common Criteria part 3 [2].

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.2. Note that all these subjects are acting for homonymous external entities. All used objects are defined either in section 9 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [1]. The operation “load” is synonymous to “import” used in [1].

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [12], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [12], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [12], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [12], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [12], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [12], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [12], A.5.1)

The following table provides an overview of the keys and certificates used:

Name	Certificate Data
CVCA Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
CVCA Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [12] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Active Authentication Key Pair	The Active Authentication asymmetric Key Pair (KPr_{AA}, KPu_{AA}) is used for the Active Authentication Protocol: allowing the chip to be authenticated as genuine by the inspection system.
Active Authentication Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to be authenticated as a genuine MRTD's chip by the inspection system. It is part of the TSF data.
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
PACE Session Keys (PACE-KMAC, PACE-KENC)	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol.

Name	Certificate Data
PACE authentication ephemeral key pair (ephem-SKPICC-PACE, ephem-PKPICC-PACE)	The ephemeral PACE Authentication Key Pair (ephem-SKPICC-PACE, ephem-PKPICC-PACE) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03110.
Ephem-PKPICC-PAC	PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 (or EF.CardSecurity) Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging TDES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging TDES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Application note: *The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if*

it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.1 TOE Security Functional Requirements

Extensions to the Security Functional Requirements from the PPs [5] [6] are defined in the subsequent section

Refinements of the security requirements are denoted in such way that added words are in **bold underline text** and removed words are ~~strikethrough~~.

6.1.1 Security Audit (FAU)

6.1.1.1 Audit Storage (FAU_SAS.1)

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

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

6.1.2 Cryptographic support (FCS)

Function		Algorithm	Key Size(s)
Chip Authentication	Hashing	SHA-1	-
	Authentication	DH	1024, 1536, 2048, 4096 bits
		ECDH	(NIST) 192, 224, 256, 320, 384, 521 bits (Brainpool) 192, 224, 256, 320, 384, 512 bits
PACE	Authentication	DH-GM	1024, 1536, 2048, 4096 bits
		ECDH-GM	(NIST) 192, 224, 256, 320, 384, 521 bits (Brainpool) 192, 224, 256, 320, 384, 512 bits
Terminal Authentication	Signature verification	RSA Pad: PKCS#1 (v1.5 [7] or PSS [24]) Hash: SHA-1, SHA-256	1024, 1280, 1536, 2048, 4096 bits
		ECDSA Hash: SHA-1, SHA-224, SHA-256	192, 224, 256, 384, 521 bits
Active Authentication	Signature generation	RSA ISO9796-2 scheme 1	1024, 1280, 1536, 2048, 4096 bits
		ECDSA Hash: SHA-1, SHA-224, SHA-256	192, 224, 256, 384, 521 bits
Secure Messaging	ENC/DEC	TDES CBC [23]	112 bits
		AES	128, 192, 256 bits
	MAC	Retail MAC	112 bits
		CMAC 8	-

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

→ Chip Authenticate 1 keys generation

FCS_CKM.1.1/ CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Diffie-Hellman key derivation Protocol compliant to PKCS#3 [20], or ECDH compliant to TR03111[17]* and specified cryptographic key sizes *DH 1024-1536-2048-4096 bits or ECDH NIST curves 192-224-256-320-384-521 bits or ECDH Brainpool curves 192-224-256-320-384-512 bits respectively* that meet the following: *TR03110-1 [12]*.

Application note: *The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol v1, see TR03110-1 [12]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [20]) or on the ECDH compliant to TR03111 [17] (i.e. an elliptic curve cryptography algorithm). The shared secret value is used to derive the CA1 session key used for encryption and MAC computation of secure messaging according to key derivation function defined in TR03110-1 [12] and for the TSF required by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC.*

→ PACE & Chip Authenticate 2 keys generation

FCS_CKM.1.1/ DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3 [20], or ECDH compliant to TR03111 [17]* and specified cryptographic key sizes *DH 1024-1536-2048-4096 bits or ECDH Generic Mapping NIST curves 192-224-256-320-384-521 bits or ECDH Generic Mapping Brainpool curves 192-224-256-320-384-512 bits respectively* that meet the following: ***TR03110-2 [13]***

Application note: *For PACE-PIN and PACE-PUK the key lengths are limited to 256, 384 and 512 bits.*

Application note*: In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is changed to TR03110-2 [13], whereas the PACE PP [6] references the ICAO-SAC specification [16]. The difference between the two definitions is that TR03110-2 [13] defines additional optional parameters for the command MSE:Set AT. These optional parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2 (TA2) can be executed right after PACE (see FIA_UID.1/PACE). As the ICAO-SAC specification [16] does not consider TA2, no such definition is given there. These additional parameters are optional and not used during PACE itself (only afterwards). If PACE is run without TA2 afterwards, access to data on the chip is given as specified by the PACE PP [6]. If TA2 is run afterwards, access to data on the chip can be further restricted w.r.t. to the authorization level of the terminal. Therefore, this change of references does not violate strict conformance*

to the PACE PP [6]. We treat this change of references as a refinement operation, and thus mark the changed reference using bold text.

***Application note**: The PACE PP [6] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to implement Chip Authentication 2 (cf. FIA_API.1/CAP2), here FCS_CKM.1/DH_PACE applies for CA2 as well.*

→ Cryptographic Key Pair generation

FCS_CKM.1.1/ KP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA and ECC key pair generation* and specified cryptographic key sizes *RSA 1024-1280-1536-2048-4096 bits or EC 192-224-256-384-521 bits respectively* that meet the following: *IEEE 1363 [24]*.

***Application note:** The component FMT_MTD.1/PK applies to both the Active Authentication Private Key and the Chip Authentication Private Key. This component defines an operation "create" that means here that these keys are generated by the TOE itself. This resulted in this instantiation of the component FCS_CKM.1 as SFR for the generation of these two keys.*

→ Secure Personalization Keys generation

FCS_CKM.1.1/ GPSCP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES key derivation* and specified cryptographic key sizes *128, 192, 256 bits* that meet the following: *GP_SPE_014 [9]*

6.1.2.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *none*.

***Application note:** The TOE destroys the BAC Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication 1 or 2 Protocol. The TOE destroys the Chip Session Keys after detection of an error in a received command by verification of the MAC. The TOE destroys the SCP03 Secure Channel Session Keys after detection of an error in a received command by verification of the MAC, and after termination of the Secure Channel. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new power-on-session.*

6.1.2.3 Cryptographic operation (FCS_COP.1)

→ Hashing

FCS_COP.1.1/	The TSF shall perform *hashing* in accordance with a specified

SHA	cryptographic algorithm *SHA-1, SHA-224 or SHA-256* and cryptographic key sizes *none* that meet the following: *FIPS 180-2 [22].*

Application note: *The Chip Authentication 1 & 2 Protocols use SHA-1 (cf. TR03110-3 [14]). For Terminal Authentication 1 & 2, the TOE shall implements either SHA-1 or additional hash function SHA-224 and SHA-256 (cf. TR03110-3 [14]). SHA-224 is supported by the TOE for ECDSA Signature operations only.*

→ SM Encrypt/Decrypt Chip Authentication 1

FCS_COP.1/ CA_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *AES and TDES in CBC mode* and cryptographic key sizes *112 bits for TDES and 128, 192, 256 bits for AES* that meet the following: *FIPS 46-3 (TDES) [23], FIPS 197 (AES) [26], and TR-03110-1 [12]*.

Application note: *The TOE implements the cryptographic primitives (e.g. TDES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol according to the FCS_CKM.1. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the symmetric authentication mechanism.*

→ SM – MAC Chip Authentication 1

FCS_COP.1/ CA_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *Retail MAC (DES) and CMAC (AES)* and cryptographic key sizes *112 for retail MAC and 128, 192 and 256 bit for CMAC* that meet the following: *[16], FIPS PUB 46-3 Data Encryption Standard (DES) [23] and [25]*.

Application note: *The TOE implements the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol according to the FCS_CKM.1/CA. Furthermore, the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.*

→ Signature verification

FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm *RSA or ECDSA* and cryptographic key sizes *RSA 1024-1280-1536-2048-4096 bits or ECDSA 192-224-256-384-521 bits respectively* that meet the following: *PKCS#1 v1.5 [7] or PKCS#1 PSS [24] and FIPS 180-2 [22]*.

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

Application note: *This SFR is concerned with Terminal Authentication 1 and 2 (see TR03110-1 [12] and TR03110-2 [13]).*

→ Signature generation

FCS_COP.1.1/ SIG_GEN	The TSF shall perform *digital signature generation* in accordance with a specified cryptographic algorithm *RSA or ECDSA* and cryptographic key sizes *RSA 1024-1536-2048-4096 bits in case of RSA and 192, 224, 256, 384 and 521 bits in case of ECFDS* that meet the following: *ISO/IEC 9796-2 [19] and ANSI x9.62 [34] respectively*.

Application note: *For signature generation in the Active Authentication mechanism, the TOE uses ISO/IEC 9796-2 compliant cryptography (scheme 1).*

→ SM Encrypt/Decrypt PACE & Chip Authentication 2

FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *AES and TDES in CBC mode* and cryptographic key sizes *112 bits (for TDES)* and *128, 192 and 256 bits (for AES)* that meet the following: : *FIPS 46-3 [23], NIST [26], TR-03110-3 [14], and [16]*.

Application note: *This SFR requires the TOE to implement the cryptographic primitive DES and AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol (PACE-KEnc) or Chip Authentication 2 (CA-KEnc) according to FCS_CKM.1/DH_PACE. The PP/ST writer has to fill in appropriate – as specified in [TR03110-3] – key sizes for AES).*

Application note: *Refinement of FCS_COP.1.1/PACE_ENC, since here PACE must adhere to [TR03110-3]. All references (both the one in [PACEPP] and [TR03110-3]) itself reference [ISO7816-4] for secure messaging. [TR03110-3] however further restricts the available choice of key-sizes and algorithms. Hence, [TR03110-3] is fully (backward) compatible to the reference given in [PACEPP].*

→ SM – MAC PACE & Chip Authentication 2

FCS_COP.1.1/ PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *CMAC and Retail MAC* and cryptographic key sizes *112, 128, 192 and 256 bits* that meet the following*[16], FIPS PUB 46-3 Data Encryption Standard (DES) [23] and [25], [14], NIST [26] and [27].*

Application note: *Refinement of FCS_COP.1.1/PACE_MAC, since here PACE must adhere to [TR03110-3]. All references (both the one in [PACEPP] and [TR03110-3]) itself reference [ISO7816-4] for secure messaging. [TR03110-3] however further restricts the available choice of key-sizes and algorithms. Hence, [TR03110-3] is fully (backward) compatible to the reference given in [PACEPP].*

→ SM GP SCP – Mutual Authentication

FCS_COP.1.1/ GPSCP_AUTH	The TSF shall perform *Mutual Authentication* in accordance with a specified cryptographic algorithm *AES cryptogram generation* and cryptographic key sizes *128, 192 and 256 bits* that meet the following *GPC_SPE_014 [9].*

→ SM GP SCP – Message Integrity & Authentication

FCS_COP.1.1/ GPSCP_MAC	The TSF shall perform *Message Authentication* in accordance with a specified cryptographic algorithm *AES CMAC* and cryptographic key sizes *128, 192 and 256 bits* that meet the following *GPC_SPE_014 [9], and NIST 800-38B [27].*

→ SM GP SCP – Message Confidentiality

FCS_COP.1.1/ GPSCP_ENC	The TSF shall perform *Message Encryption & Decryption* in accordance with a specified cryptographic algorithm *AES CBC* and cryptographic key sizes *128, 192 and 256 bits* that meet the following *GPC_SPE_014 [9], and FIPS 197 [26].*

6.1.2.4 Random Number Generation (FCS_RND.1)

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *AIS31 class "P2 – SOF-High"*.

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

6.1.3 Identification and authentication (FIA)

The following table provides an overview on the authentication mechanisms used:

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol 1	FIA_API.1/CAP FIA_UAU.5/PACE FIA_UAU.6/EAC
Chip Authentication Protocol 2	FIA_API.1/CAP2 FIA_UAU.5/PACE FIA_UAU.6/CA
Terminal Authentication Protocol 1 & 2	FIA_UAU.1_PACE FIA_UAU.5_PACE
Active Authentication Protocol	FIA_API.1/AAP
PACE protocol	FIA_UAU.1/PACE FIA_UAU.4/PACE FIA_UAU.5/PACE FIA_UAU.6/PACE FIA_AFL.1/PACE FIA_API.1/CA FIA_API.1/CAP FIA_API.1/CAP2
Mutual Authentication for GP SCP03	FIA_UID.1/GPSCP FIA_UAU.1/GPSCP

Note: the Chip Authentication Protocol 1 as defined in the PP [5] includes:

- the BAC authentication protocol as defined in ‘ICAO Doc 9303’ [11] in order to gain access to the Chip Authentication 1 Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication 1 Public Key and the Terminal Public Key used later in the Terminal Authentication 1 Protocol,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The BAC mechanism does not provide a security function on its own. The Chip Authentication 1 Protocol may be used independent of the Terminal Authentication 1 Protocol. But if the Terminal Authentication 1 Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol 1.

This does not apply for EAC2 as in that case, the TA2 is necessarily performed just after PACE and only after that the CA2 can be performed.

6.1.3.1 Authentication Failure Handling (FIA_AFL.1)

→ FIA_AFL.1/PACE

FIA_AFL.1.1/ PACE	The TSF shall detect when a *1* unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.
FIA_AFL.1.2/ PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall *send the response to the authentication request with exponentially increasing time delays until the correct password is used*

***Application Note**: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [16]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy, the TOE shall not allow a quick monitoring of its behavior (e.g. due to a long reaction time) in order to make the first step of the skimming attack requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP. One of some opportunities for performing this operation might be "consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords".*

***Application Note**: The count of consecutive unsuccessful authentications is stored in non-volatile memory and is preserved across power-up and power-down cycles. After a successful authentication the count is reset to zero.*

Refined SFR relevant for configuration "eDigitalIdentity"

The SFR FIA_AFL.1/PACE defined in this section is only applicable for configuration "eDigitalIdentity" and replaces respective claim at the beginning of this section.

→ FIA_AFL.1/PACE

FIA_AFL.1.1/ PACE	The TSF shall detect when a [**Number**] unsuccessful authentication attempt occurs related to [**Authentication events**].
FIA_AFL.1.2/ PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**Actions**].

Password	Number	Authentication events	Actions
MRZ, CAN	1	Authentication attempts using the PACE password (MRZ, CAN) as shared password	Exponentially increase time delay before new authentication attempt is possible.
CAN	[0-255: number of presentations]	Authentication attempt involving CAN as shared password for PACE	Wait for an increasing time between receiving of the terminal challenge and sending of the TSF response during the PACE

			authentication attempts.
PIN & PUK	An administrator configurable positive integer linked to the size of the PIN or PUK (respectively)	Consecutive failed authentication attempts using the PIN or PUK as the shared password for PACE leaving a single authentication attempt.	Suspend the PIN or the PUK
	1	On suspend mode, a bad or correct value presentation attempts using the PIN or PUK as the shared password for PACE.	Suspend the PIN or the PUK
	1	On suspend mode, after a PACE CAN authentication, a bad PIN / PUK value presentation attempt.	Block the PIN or the PUK

Application note: *The refinement rules out several actions which do not decrease security and thus is in conformance with [6].*

6.1.3.2 Timing of identification (FIA_UID.1)

FIA_UID.1.1/PACE The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to TR-03110-2 [13]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol v.1 according to TR03110-1 [12]
5. to carry out the Terminal Authentication Protocol v.1 according to TR03110-1 [12]
6. *carrying out the Terminal Authentication protocol 2 according to TR-03110-2 [13]*
7. *to carry out the Active Authentication Mechanism*

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

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

***Application Note**: In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE. The manufacturer writes the initialization data and/or pre-personalization data in the audit records of the IC. Note that a personalization agent acts on behalf of the electronic document issuer under his and the CSCA's and DS's policies. Hence, they define authentication procedures for personalization agents. The TOE must functionally support these authentication procedures. These procedures are subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role personalization agent, if a terminal proves the respective Terminal Authorization level (e. g. a privileged terminal, cf. TR03110-2 [13]).*

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

***Application note:** The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2 terminals are application dependent;**Application Note:** The SFR FIA_UID.1/PACE in this ST covers the definition in the EAC1 and EAC2 PP that, in turn, extends the definition in the PACE PP by EAC aspect 4 to 6. This extension does not conflict with the strict conformance to PACE PP.*

FIA_UID.1.1/GPSCP	The TSF shall allow 1. *to establish the communication channel*, 2. *carrying out the Mutual Authentication Protocol according to GP_SPE_014 [9]* on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/GPSCP	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

***Application Note**: The user in that case is the user having knowledge of the static SCP03 keys allowing the initiation of the SCP (typically the Manufacturer, Pre-personalizer, Personalizer, …).*

6.1.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to TR-03110-2 [13], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to identify themselves by selection of the authentication key, 5. to carry out the Chip Authentication Protocol Version 1 according to [12],

6. to carry out the Terminal Authentication Protocol Version 1 according to [12],
7. *carrying out the Terminal Authentication protocol 2 according to TR-03110-2 [13],*
8. *to carry out the Active Authentication mechanism*

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

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

***Application Note**: The SFR FIA_UAU.1/PACE in this ST covers the definition in the EAC1 and EAC2 PP that, in turn, extends the definition in the PACE PP by EAC aspect 5 to 7. This extension does not conflict with the strict conformance to PACE PP.*

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

***Application Note**: The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated terminal will immediately perform Chip Authentication 2 as required by FIA_API.1/CAP2 using, amongst other, Comp(ephem-PKPCD-TA) from the accomplished TA2. Note that Passive Authentication using SOC is considered to be part of CA2 within this PP.*

FIA_UAU.1.1/GPSCP The TSF shall allow

1. *to establish the communication channel*,
2. *carrying out the Mutual Authentication Protocol according to GP_SPE_014 [9],*

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

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

***Application Note**: The user in that case is the user having knowledge of the static SCP03 keys allowing the initiation of the SCP (typically the Manufacturer, Prepersonalizer, Personalizer).*

6.1.3.4 Single-use authentication mechanisms (FIA_UAU.4)

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

1. PACE protocol,
2. Terminal Authentication 1 Protocol,

3. Authentication Mechanism based on *AES and TDES,*
4. *Terminal Authentication 2 protocol according to TR-03110-2 [13]*
5. *Active Authentication Protocol*.

Application note: *The SFR FIA_UAU.4.1 in this ST covers the definition in the EAC1 and EAC2 PP [5] that, in turn, extends the definition in PACE PP by the EAC aspect 3 & 4. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from PACE PP.*

Application note: *For TA2, the TOE randomly selects a nonce rPICC of 64bit length, see TR03110-2 [13]. This SFR extends FIA_UAU.4/PACE from PACE PP [6] by assigning the authentication mechanism Terminal Authentication 2.*

6.1.3.5 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE protocol
2. Passive authentication
3. Terminal Authentication 1 Protocol,
4. Secure messaging in MAC-ENC mode,
5. Symmetric Authentication Mechanism based on *TDES and AES*
6. *Terminal Authentication 2 protocol according to TR-03110-2 [13],*
7. *Chip Authentication 2 according to TR-03110-2 [13],*

to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent by *the Symmetric Authentication Mechanism with Personalization Agent Key*.
2. The TOE accepts the authentication attempt as Travel Document Manufacturer by *the Authentication Mechanism with Travel Document Manufacturer Keys*
3. 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

4. After run of the Chip Authentication Protocol 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.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol 1 only if the terminal uses the public key presented during the Chip Authentication Protocol 1 and the secure messaging established by the Chip Authentication Mechanism 1
6. *The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol only if (i) the terminal presents its static public key PK_{PCD} and the key is successfully verifiable up to CVCA and (ii) the terminal uses the PICC identifier ID_{PICC} = Comp(ephem-PK_{PICC}-PACE) calculated during, and the secure messaging established by the, current PACE authentication.*
7. *Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct massage authentication codes sent by secure messaging with the key agree with the terminal by Chip Authentication 2.*

Application note: *Depending on the authentication methods used the Personalization Agent holds a key for the Symmetric Authentication Mechanism. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.*

Application note: *Note that 6. and 7. in FIA_UAU.5.1/PACE and 6. and 7. of FIA_UAU.5.2/ PACE are additional assignments (using the open assignment operation) compared to PACE PP [6].*

6.1.3.6 Re-authenticating (FIA_UAU.6)

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 shall be verified as being sent by the GIS.

Application note: *The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [11] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.*

FIA_UAU.6.1/CA The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication 2 shall be verified as being sent by the EAC2 terminal.

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.

Application note: *The PACE protocol specified in [16] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.*

6.1.3.7 Authentication Proof of Identity (FIA_API.1)

→ Chip Authentication Protocol v1

FIA_API.1.1/CAP The TSF shall provide a Chip Authentication Protocol 1 according to [12] to prove the identity of the TOE.

Application note: *This SFR requires the TOE to implement the Chip Authentication 1 Mechanism specified in TR03110-1 [12]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [11],. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication 1 Private Key corresponding to the Chip Authentication 1 Key (EF.DG14).*

→ Chip Authentication Protocol v2

FIA_API.1.1/ CAP2	The TSF shall provide the protocol Chip Authentication 2 Protocol according to TR-03110-2 [13] to prove the identity of the TOE.

Application note: *This SFR corresponds to the SFR named FIA_API.1/CA in PP0086 [39]. It was renamed FIA_API.1/CAP2 in the current ST by similarity with FIA_API.1/CAP that addresses Chip Authentication 1 Protocol.*

→ Active Authentication Protocol

FIA_API.1.1/ AAP	The TSF shall provide an *Active Authentication Protocol according to [11]* to prove the identity of the *TOE*.

Application note: *The TOE may implement the Active Authentication Mechanism specified in [11] Part 1 Appendix 4 to section IV. This mechanism is a challenge response protocol where TOE challenge response is calculated being digital signature over the terminal's 8 bytes nonce.*

Additional Iteration relevant for configuration "eDigitalIdentity"

The SFR FIA_API.1/CA defined in this section adds an additional iteration of FIA_API.1 and is only applicable for configuration "eDigitalIdentity".

→ eDigitalIdentity authentication mechanism

FIA_API.1.1/ CA	The TSF shall provide an authentication mechanism to prove the identity of the eDigitalIdentity holder.

Application note: *The TOE acts as a substitute for the eDigitalIdentity document holder, to authenticate digitally on its behalf. The authentication mechanism is triggered by the eDigitialIdentity Document holder itself by presenting its PIN to the TOE.*

6.1.4 User data protection (FDP)

6.1.4.1 Subset access control (FDP_ACC.1)

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

Refined SFR relevant for configuration "eDigitalIdentity"

The SFR FDP_ACC.1/TRM defined in this section is only applicable for configuration "eDigitalIdentity" and replaces respective claim at the beginning of this section.

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

Application note: *The refinement is of terminological nature only, hence the strict conformance is not violated by this syntactical change.*

6.1.4.2 Security attribute based access control (FDP_ACF.1)

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

3. Subjects:
   a. BIS-PACE,
   b. Extended Inspection System
   c. Terminal,
4. Objects:
   a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical MRTD,
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document,
5. Security attributes:
   a. PACE authentication
   b. authentication status of terminals,
   c. Terminal Authentication.

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 TR-03110-2 [13] after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

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

1. 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
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application note: *The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [12], Annex A.5.1, table A.8. 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.*

Application Note*: The SFR FDP_ACF.1.1/TRM in this ST covers the definition in the EAC PP [5] that, in turn, extends the definition in PACE PP [6] by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [6]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in the EAC PP [5] that, in turn, extends the definition in PACE PP [6] by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP*

Application Note: *FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).*

Application Note*: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.*

FDP_ACF.1.1/ TRM2	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Terminal, b. PACE terminal, c. EAC2 terminal 2. Objects: a. All user data stored in the TOE; including sensitive data, b. all TOE intrinsic secret (i.e. cryptographic) data. 3. Security attributes: a. Terminal Authentication Level (access rights)
FDP_ACF.1.2/ TRM2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM according to TR-03110-2 [13] as required by FIA_UAU.1/PACE.
FDP_ACF.1.3/ TRM2	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: noneEAC.

FDP_ACF.1.4/TRM2 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. Any terminal not being a PACE terminal or an EAC2 terminal is not allowed to read, to write, to modify, or to use any User Data stored on the electronic document
2. Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document
3. No subject is allowed to read “Communication Establishment Authorization Data’ stored on the electronic document.
4. No subject is allowed to write or modify ‘secret electronic document holder authentication data’ stored on the electronic document, except for PACE terminals or EAC2 terminals executing PIN management based on the following: [assignment: list of rules for PIN management chosen from TR03110-2 [13]]
5. No subject is allowed to read, write, modify, or use the private Chip Authentication key(s) stored on the electronic document
6. Reading, modifying, writing, or using sensitive user data is only allowed to EAC2 terminals using the following mechanism:

   The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to TR03110-2 [13]. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean ‘and’ of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.
7. No subject is allowed to read, write, modify, or use the data objects 2b) of FDP_ACF.1.1/TRM2

Application note: *The above definition covers FDP_ACF.1.1/TRM from PACE PP [6] and extends it by additional subjects and objects. Below we justify all refinements: In FDP_ACF.1 1b) a refinement is used to replace the term BIS-PACE with PACE-Terminal as specified in Table 1. Such syntactic change does not violate strict conformance. Subject 1c) is added by applying the open assignment operation (4) from PACE PP [6]. Next, data objects 2a), b) and c) of PACE PP [6] are here generalized from a specific enumeration to all user data stored on the TOE as bullet point 2a) above using a refinement. Since this includes all data defined in PACE PP [6] (DG3 and DG4 are sensitive data; the other DG's of PACE PP [6] are common user*

data), this does not violate strict conformance. For 2b) in this PP the open assignment (4) of PACE PP [6] is used to add an additional object. The term authentication status of terminals (3a) is here refined to terminal authentication level, since the former term is simply very imprecise for a TOE implementing Terminal Authentication. In FDP_ACF.1.2/TRM, besides the aforementioned renaming of terminology (a simple syntactic change without changing semantics), a reference is changed. For that reference, Application Note 10 applies. For FDP_ACF.1.4/TRM rule 1, a slight refinement of wording ("not being" vs "being not") is made to increase clarity, and terms are replaced according to Table 1. This is however again just a syntactic correction without changing the semantics. In addition, the subject EAC2-Terminal is added. Since an EAC2-Terminal must be authenticated by executing PACE prior to be given access, this does not decrease security and thus is in conformance with PACE PP [6]. Rule 2 is refined by applying Table 1. This syntactic replacement of terminology does also not violate strict conformance. The remaining rules 4-7 are additional assignments using the open assignment operation from PACE PP [6]. Note that rule 4) narrows down the open assignment ([CC1], 8.1.2 c) of PACE PP [6] by leaving itself an open assignment of PIN management rules.

***Application Note**: Note that here, all sensitive user data are assumed to be protected by EAC2 (cf. FIA_UAU.5). If this PP is claimed, the definition of sensitive user data may distinguish between different kinds of sensitive user data, where some are protected by EAC2, and some are protected by an equivalent (in terms of the security level) security mechanism, such as EAC1*

Refined SFR relevant for configuration "eDigitalIdentity"

The SFR FDP_ACF.1/TRM defined in this section is only applicable for configuration "eDigitalIdentity" and replaces respective claim at the beginning of this section.

FDP_ACF.1.1/TRM — The TSF shall enforce the Access Control SFP to objects based on the following:

1. Subjects:
   - **a. PACE terminal**
   - b. Extended Inspection System
   - c. Terminal,
2. Objects:
   - a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical **eDigitalIdentity document**,
   - b. data in EF.DG3 of the logical **eDigitalIdentity document**,
   - c. data in EF.DG4 of the logical **eDigitalIdentity document**,
   - d. all TOE intrinsic secret cryptographic keys stored in the **eDigitalIdentity** document,
3. Security attributes:
   - a. PACE **PIN** authentication
   - b. authentication status of terminals,
   - c. Terminal Authentication.
   - **d. Chip Authentication v1.**

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 **PACE Terminal** is allowed to read data objects from FDP_ACF.1.1/TRM according to [16] after **at least** successful PACE authentication as required by FIA_UAU.1/PACE.
- **A PACE Terminal is allowed to read data objects 2a) of FDP_ACF.1.1/TRM according to [38] only after a successful PACE authentication followed by Chip Authentication v1 as required by FIA_UAU.1/PACE. This rule is not applicable for EF.DG14.**
- **A PACE Terminal is allowed to read data objects 2b) and 2c) of FDP_ACF.1.1/TRM according to [38] only after a successful PACE authentication followed by Chip Authentication v1 and Terminal Authentication v1 as required by FIA_UAU.1/PACE.**

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

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

1. Any terminal being not authenticated **at least** as PACE authenticated **PACE Terminal** is not allowed to read, to write, to modify, to use any User Data stored on the **eDigitalIdentity Document**
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the **eDigitalIdentity Document**
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 ~~**(Fingerprint)**~~ granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 ~~**(Iris)**~~ granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application note: *Contrarily to ePP configuration, in eDI configuration the data objects can be read only after PACE followed by Chip Authentication v1.*

Application note: *Below we justify all refinements: In FDP_ACF.1.1 1a) a refinement is used to replace the term BIS-PACE with PACE terminal. Such syntactic change does not violate strict conformance. In FDP_ACF.1.1 2) a refinement is used to replace the term travel document with eDigitalIdentity document. Such syntactic change does not violate strict conformance. In FDP_ACF.1.1 3d) the Chip Authentication v1 is added as new attribute. For FDP_ACF.1.2, the added term "at least" of rule 1 with the remaining rules 2 and 3 does not decrease security and this is in conformance with [5][6]. For FDP_ACF.1.4 rule 1, the added word "at least" does not decrease security and this is in conformance with [5][6].*

6.1.4.3 Residual Information Protection (FDP_RIP.1)

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* the following objects.

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem-SKPICC-PACE (by having generated a DH shared secret K).

Additional iterations relevant for configuration "eDigitalIdentity"

FDP_RIP.1.1 / PINPUK	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects. 3. PIN and PUK
FDP_RIP.1.1 / CASS	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects. 4. Replaced Chip Authentication Security Service

6.1.4.4 Basic data exchange confidentiality (FDP_UCT.1)

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

6.1.4.5 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/ TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.
FDP_UIT.1.2/ TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred.

6.1.5 Security Management (FMT)

6.1.5.1 Specifications of Management Functions (FMT_SMF.1)

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-personalization, 3. Personalization, 4. Configuration.

Additional iterations relevant for configuration “eDigitalIdentity”

FMT_SMF.1.1 / PINPUK	The TSF shall be capable of performing the following security management functions: 5. Initialize and resume the PIN or the PUK 6. Change and unblock the PIN
FMT_SMF.1.1 / CASS	The TSF shall be capable of performing the following security management functions: 7. Replace Chip Authentication Security Service

6.1.5.2 Security roles (FMT_SMR.1)

FMT_SMR.1.1/ PACE — The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal
4. PACE authenticated BIS-PACE
5. *Country Verifying Certification Authority,*
6. *Document Verifier,*
7. *Domestic Extended Inspection System*
8. *Foreign Extended Inspection System.*
9. *Basic Inspection System*
10. *EAC2 terminal*
11. *Electronic document Holder*

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

***Application Note**: The SFR FMT_SMR.1.1/PACE in this ST covers the definition in the EAC1 and EAC2 PP that, in turn, extends the definition in PACE PP by 5) to 11). This extension does not conflict with the strict conformance to PACE PP.*

***Application note:** For explanation on the role Manufacturer and Personalization Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the travel document presenter).*

The TOE recognises the travel document holder or an authorised other person or device (BIS-PACE) by using PACE authenticated BIS-PACE (FIA_UAU.1/PACE).

***Application Note**: The role terminal is the default role for any terminal being recognized by the TOE as neither PACE terminal nor EAC1 nor EAC2 terminal. The roles CVCA, DV, and EAC2 terminal are recognized by analyzing the current Terminal Certificate, cf. TR03110-2 [13], (FIA_UAU.1/PACE). Specific types of EAC2 terminals are identified analogously. The TOE recognizes the electronic document holder by using a PACE terminal together with inputs PIN or PUK (FIA_UAU.1/PACE). Here FMT_SMR.1.1 covers FMT_SMR.1.1/PACE in PACE PP [16] and assigns additional roles 10 and 11 for EAC2 as in PP0086.This extension does not conflict with the strict conformance to PACE PP [16].*

6.1.5.3 Limited capabilities (FMT_LIM.1)

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

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be manipulated and disclosed,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

6.1.5.4 Limited availability (FMT_LIM.2)

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

Deploying Test Features after TOE Delivery does not allow,

1. User Data to be manipulated and disclosed,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

Application note: *The formulation of "Deploying Test Features …" in FMT_LIM.2.1 is very misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*

Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.1.5.5 Additional SFRs relevant for "eDigitalIdentity": Management of security functions behavior (FMT_MOF.1)

→ Updating Chip Authentication Security Services

FMT_MOF.1.1/ CASS The TSF shall restrict the ability to modify the behavior of the function Chip Authentication to the Personalization Agent.

Application note: *By updating the Chip Authentication Key type, the algorithm used for Chip Authentication will be modified accordingly (see FMT_MTD.1.1/CASS)*

6.1.5.6 Management of TSF data (FMT_MTD.1)

→ Writing of Initialization Data and Pre-personalization Data

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

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

→ Disabling of Read Access to Initialization Data and Pre-personalization Data

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to read out the Initialization Data and the Pre-personalization Data to the Personalization Agent.

Application note: *According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.*

→ Initialization of CVCA Certificate and Current Date

FMT_MTD.1.1/ CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date to *the Personalization Agent*.

Application note: *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [12], section 2.2.6). 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.*

→ Country Verifying Certification Authority

FMT_MTD.1.1/ CVCA_UPD — The TSF shall restrict the ability to update the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate,

to Country Verifying Certification Authority.

Application note: *The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [12], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link- Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [12], sec. 2.2.3 and 2.2.4).*

→ Current date

FMT_MTD.1.1/ DATE — The TSF shall restrict the ability to modify the Current date to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System.
4. *EAC2 terminal possessing an accurate Terminal Certificate according to TR03110-3 [14]*

Application note: *The authorized roles are identified in their certificate (cf. [12], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [12], annex A.3.3, for details).*

Application note: *The authorized roles are identified in their certificates (cf. TR03110-2 [13]) and are authorized by validating the certificate chain up to the CVCA (cf. FMT_MTD.3). The authorized role of a terminal is part of the Certificate Holder Authorization in the card verifiable certificate that is provided by the terminal within Terminal Authentication 2 (cf. TR03110-3 [14]). Different types of EAC2 terminals may exist, cf. TR03110-2 [13]. They need to be defined, i.e. assigned in FMT_SMR.1 by the PP/ST writer.*

→ Key Write

FMT_MTD.1.1/ KEY_WRITE — The TSF shall restrict the ability to *write* the *Document Basic Access Keys* to *the Personalization Agent*.

Application note: *The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.*

→ Chip Authentication Private Key

FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to *create or load* the Chip Authentication 1&2 Private Key to *the Personalization Agent*.

Application note: *The component FMT_MTD.1/CAPK was refined in this Security Target by selecting both "create" and "load" operations. The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory: the generator, the modulus and the order. The verb "create" means here that the Chip Authentication Private Key order is generated by the TOE itself. See the instantiation of the component FCS_CKM.1/PK as SFR for this key generation.*

Application note: *Chip Authentication 1&2 Private Key stands for active Private Key or pre-created replacement Private Keys.*

→ Active Authentication Private Key

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to *load* the *Active Authentication Private Key* to *the Personalization Agent*.

Application note: *The "load" option is selected here and may be used by the successfully authenticated Personalization Agent if he is willing to include the optional Active Authentication Key in the MRTD. The verb "load" means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory.*

→ Personalization agent

FMT_MTD.1.1/ PA	The TSF shall restrict the ability to write the SOC & SOD to the Personalization Agent

Application note: *Note that the card/chip security objects (SOC) are mentioned here in addition to SOD. These contain information, such as algorithm identifiers, only necessary for EAC2. All requirements formulated in PACE PP [16] are thus met, and strict conformance is therefore not violated.*

→ Key Read

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the 1. PACE passwords 2. Chip Authentication 1 Private Key, 3. Personalization Agent Keys 4. *Active Authentication Private Key* 5. *Chip Authentication 2 Private Key(s) (SK_{PICC})*

to none.

Application note: *Chip Authentication 1 or 2 Private Key stands for active Private Key or pre-created replacement Private Keys*

Application note: *FMT_MTD.1/KEY_READ extends the SFR from PACE PP [16] by additional assignments for EAC2 (as in PP0086) and Active Authentication*

Additional iterations relevant for configuration "eDigitalIdentity"

→ Initialize PIN or PUK

FMT_MTD.1.1/ Initialize_PINPUK	The TSF shall restrict the ability to write the initial PIN and PUK to the personalization agent.

→ Resume PIN or PUK

FMT_MTD.1.1/ Resume_PINPUK	The TSF shall restrict the ability to resume the suspended PIN or the PUK to the electronic document holder.

Application Note*: This SFR holds for any electronic document holder in particular for the eDigitalIdentity document holder.*

→ Change PIN

FMT_MTD.1.1/ Change_PIN	The TSF shall restrict the ability to change the PIN to the electronic document holder.

Application Note*: This SFR holds for any electronic document holder in particular for the eDigitalIdentity document holder.*

→ Unblock PIN

FMT_MTD.1.1/ Unblock_PIN	The TSF shall restrict the ability to unblock the blocked PIN to the electronic document holder (using the PUK for unblocking).

Application Note*: This SFR holds for any electronic document holder in particular for the eDigitalIdentity document holder.*

FMT_MTD.1.1/ Unblock_PIN2	The TSF shall restrict the ability to unblock the blocked PIN to an EAC2 terminal of a type that has the terminal authorization level for PIN management.

Application Note*: The unblocking procedure must be implemented according to TR03110-2 [16], and is relevant for the status as required by FIA_AFL.1/PACE. It can*

be triggered by either (i) the electronic document holder being authenticated as required by FIA_UAU.1/PACE using the PUK as the shared password or (ii) an EAC2 terminal (FIA_UAU.1/PACE) that proved a terminal authorization level being sufficient for PIN management (FDP_ACF.1/TRM2).

→ Activate PIN

FMT_MTD.1.1/ Activate_PIN	The TSF shall restrict the ability to activate and deactivate the PIN to an EAC2 terminal of a type that has the terminal authorization level for PIN management.

***Application Note**: The activation/deactivation procedures must be implemented according to TR03110-2 [13]. They can be triggered by an EAC2 terminal (FIA_UAU.1/PACE) that proved a terminal authorization level sufficient for PIN management (FDP_ACF.1/TRM2)*.

→ Chip Authentication Security Service Replacement

FMT_MTD.1.1/ CASS	The TSF shall restrict the ability to replace the Chip Authentication 1 or 2 Security Service to the Personalization Agent.

***Application note:** By updating the Chip Authentication 1 or 2 Key type, the algorithm used for Chip Authentication 1 or 2 will be modified accordingly (see FMT_MOF.1.1/CASS)*

6.1.5.7 Secure TSF data (FMT_MTD.3)

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 1 & 2 Protocol and the Access Control. **Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to TR03110-3 [14]**

***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 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 and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.*

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

Application note: *The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.*

Application note: *Terminal Authentication is used as required by (i) FIA_UAU.1/EAC2_Terminal and FIA_UAU.5. The terminal authorization level derived from the CVCA Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access control required by FDP_ACF.1/TRM.*

6.1.6 Protection of the TSF (FPT)

6.1.6.1 TOE Emanation (FPT_EMSEC.1)

FPT_EMSEC.1.1 The TOE shall not emit *information of IC Power consumption* in excess of *State-of-the-Art values* enabling access to

1. Chip Authentication 1 Session Keys,
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),
3. The ephemeral private keys SK_{PICC} (PACE)
4. Personalization Agent Key(s)
5. Chip Authentication 1 Private Key, and
6. *Active Authentication Private Key*.
7. *Chip Authentication 2 Private Key*
8. *PIN, PUK*

FPT_EMSEC.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts *to gain* access to

1. Chip Authentication 1 Session Keys,
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),
3. The ephemeral private keys SK_{PICC} (PACE)
4. Personalization Agent Key(s),
5. Chip Authentication 1 Private Key, and
6. *Active Authentication Private Key*.

7. *Chip Authentication 2 Private Key(s) (SK_{PICC})*
8. *PIN, PUK*

Application note: *The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip provides a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.*

Application note: *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power consumption, timing of signals, and electromagnetic radiation due to internal operations or data transmissions. Note that while the security functionality described in FPT_EMSEC.1 should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development. Note that in the above SFR, all items in FPT_EMS.1.2 from 3. upwards are additional assignments. The first item is slightly refined to include CA-key(s)*

6.1.6.2 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. failure detected by TSF according to FPT_TST.1,

Additional iteration relevant for configuration "eDigitalIdentity"

FPT_FLS.1.1/ CASS	The TSF shall preserve a secure state when the following types of failures occur: 3. Failure of the CASS replacement.

6.1.6.3 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1	The TSF shall resist Physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Application note: *The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.*

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

6.1.6.4 TSF testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of self-tests *during initial start-up* to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application note: *self-test for the verification of the integrity of stored TSF executable code are executed during initial start-up in the Phase 3 "Personalization" and Phase 4 "Operational Use".*

6.1.7 Trusted Path/Channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

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

Application note: *the trusted IT product is the PACE terminal*

FTP_ITC.1.1/ CA2	The TSF shall provide a communication channel between itself and **an EAC2 terminal** 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. **The trusted channel shell be established by performing the CA2 protocol according to TR03110-2 [16].**
FTP_ITC.1.2/ CA2	The TSF shall permit **an EAC2 terminal** to initiate communication via the trusted channel.
FTP_ITC.1.3/ CA2	The TSF shall **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.

Application note: *The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE), the TA2 protocol (FIA_UAU.1/PACE) and the CA2 protocol (FIA_API.1/CAP2). If Chip Authentication 2 was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-KMAC, CA-KEnc). This secure messaging enforces the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC*.

6.2 TOE Security Assurance Requirements

TOE Security Assurance Requirements as stated in section 6.2 of the claimed PP [5].

ALC_DVS is augmented from 1 to 2, and AVA_VAN is augmented from 3 to 5, compared to the CC V3.1 package for EAL5.

6.2.1 SARs Measures

The assurance measures that satisfy the TOE security assurance requirements are the following:

Assurance Class	Component	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete Semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semi-formal modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_LCD.1	Developer defined lifecycle model
	ALC_TAT.2	Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Test	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5**	**Advanced methodical vulnerability analysis**

Table 8. Assurance Requirements: EAL5 augmented

6.2.2 SARs Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

ALC_DVS.2 Life-cycle support- Sufficiency of security measures

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

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 Vulnerability Assessment - Advanced methodical vulnerability analysis

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 fulfil the security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof and OT.AA_Proof.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

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

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

The following table associates the security requirements and the security objectives of the TOE. The security requirements of the TOE correspond to at least one security objective of the TOE. Moreover, some requirements correspond to the security objectives of the TOE in combination with other objectives.

TOE SFR / TOE Security objectives	OT.Sens_Data_Conf	OT_Sens_Data_EAC2	OT.Chip_Aut_Proof	OT.CA2	OT.AA_Proof	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Sens_Ident_User_Data_Conf	OT.CASS_Replace
FAU_SAS.1						X	X				X							
FCS_CKM.1/CA	X		X			X		X	X	X								
FCS_CKM.1/DH_PACE		X		X				X	X	X								X
FCS_CKM.1/KP					X													
FCS_CKM.1/GPSCP	X							X	X	X								X
FCS_CKM.4	X	X		X		X		X	X	X								
FCS_COP.1/CA_ENC	X		X			X		X		X								
FCS_COP.1/CA_MAC	X		X			X		X										
FCS_COP.1/SIG_VER	X					X											X	
FCS_COP.1/SIG_GEN					X	X												
FCS_COP.1/SHA		X	X	X	X			X	X	X								
FCS_COP.1/PACE_ENC		X								X								X
FCS_COP.1/PACE_MAC				X				X	X									X
FCS_COP.1/GPSCP_AUTH	X							X	X	X								X
FCS_COP.1/GPSCP_ENC	X								X	X								X
FCS_COP.1/GPSCP_MAC	X							X	X	X								X
FCS_RND.1	X	X		X	X	X		X	X	X								
FIA_UID.1/GPSCP	X							X	X	X								X
FIA_UAU.1/GPSCP	X							X	X	X								X
FIA_AFL.1/PACE		X				X	X	X	X	X				X			X	
FIA_UID.1/PACE	X	X				X	X	X	X	X								
FIA_UAU.1/PACE	X	X				X	X	X	X	X								
FIA_UAU.4/PACE	X	X				X		X	X	X								
FIA_UAU.5/PACE	X	X		X		X		X	X	X								
FIA_UAU.6/EAC	X					X		X	X	X								

TOE SFR / TOE Security objectives	OT.Sens_Data_Conf	OT_Sens_Data_EAC2	OT.Chip_Aut_Proof	OT.CA2	OT.AA_Proof	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Sens_Ident_User_Data_Conf	OT.CASS_Replace
FIA_UAU.6/CA		X						X	X	X								
FIA_UAU.6/PACE		X						X	X	X								
FIA_API.1/CAP			X															
FIA_API.1/CAP2		X		X														
FIA_API.1/AAP					X													
FIA_API.1/CA								X	X	X							X	
FDP_ACC.1/TRM	X	X				X	X	X		X							X	
FDP_ACF.1/TRM	X					X		X		X							X	
FDP_ACF.1/TRM2		X					X	X		X								
FDP_RIP.1		X		X				X	X	X								
FDP_RIP.1/PINPUK						X	X	X	X	X							X	
FDP_RIP.1/CASS																		X
FDP_UCT.1/TRM	X	X						X		X								
FDP_UIT.1/TRM		X						X		X								
FMT_SMF.1		X	X			X	X	X	X	X	X							
FMT_SMF.1/PINPUK		X				X		X	X	X							X	
FMT_SMF.1/CASS																		X
FMT_SMR.1/PACE		X	X			X	X	X	X	X	X							X
FMT_LIM.1												X						
FTM_LIM.2												X						
FMT_MOF.1/CASS																		X
FMT_MTD.1/INI_ENA						X	X				X							
FMT_MTD.1/INI_DIS						X	X				X							
FMT_MTD.1/CVCA_INI	X	X																
FMT_MTD.1/CVCA_UPD	X	X																
FMT_MTD.1/DATE	X	X						X	X	X								
FMT_MTD.1/KEY_WRITE	X					X												
FMT_MTD.1/CAPK	X	X	X	X				X	X	X								
FMT_MTD.1/CASS																		X
FMT_MTD.1/AAPK					X	X												
FMT_MTD.1/PA		X		X		X	X	X	X	X								
FMT_MTD.1/KEY_READ	X	X	X	X		X	X	X	X	X								X
FMT_MTD.1/Initialize_PINPUK		X					X	X	X	X							X	

TOE SFR / TOE Security objectives	OT.Sens_Data_Conf	OT_Sens_Data_EAC2	OT.Chip_Aut_Proof	OT.CA2	OT.AA_Proof	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Data_Int	OT.Data_Aut	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Sens_Ident_User_Data_Conf	OT.CASS_Replace
FMT_MTD.1/Resume_PINPUK		X					X	X	X	X							X	
FMT_MTD.1/Change_PIN		X					X	X	X	X							X	
FMT_MTD.1/Unblock_PIN		X					X	X	X	X							X	
FMT_MTD.1/Unblock_PIN2		X					X	X	X	X								
FMT_MTD.1/Activate_PIN		X					X	X	X	X								
FMT_MTD.3	X	X						X	X	X								
FPT_EMSEC.1						X							X					
FPT_FLS.1													X			X		
FPT_FLS.1/CASS																		X
FPT_PHP.3								X					X		X			
FPT_TST.1													X			X		
FTP_ITC.1/PACE		X						X	X	X				X				
FTP_ITC.1/CA2		X						X	X	X				X				

Table 9. Functional Requirement to TOE Security Objective Mapping

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

OT.AA_Proof (Proof of MRTD's chip authenticity by Active Authentication) is ensured by the Active Authentication Protocol provided by FIA_API.1/AAP enforcing the identification and authentication of the MRTD's chip. The Active Authentication protocol requires FCS_RND.1 (for the generation of the challenge), and FCS_COP.1/SHA (for the host challenge hashing) and FCS_COP.1/SIG_GEN (for the signature generation). The Active Authentication private Key is used. This TOE secret data is created during Personalization (Phase 3) according to FCS_CKM.1/KP (for Key Pair generation mechanism), and by authorized agent as required by FMT_MTD.1/ AAPK.

OT.AC_Pers (Access Control for Personalization of logical MRTD) addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalization Data (including Active Authentication keys generated with FCS_COP.1/SIG_GEN) loaded through FMT_MTD.1/AAPK). The write access to the logical travel document data are 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 Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMSEC.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC1 (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use. The Personalization Agent also handles the security environment object according to the SFR FMT_MTD.1/KEY_WRITE.

Additionally, in the case of eDigitalIdentity configuration, the security objective **OT.AC_Pers** is achieved by terminal identification/authentication using and managing the PIN/PUK as required by the SFRs FIA_AFL.1/PACE. The SFR FMT_SMF.1/PINPUK support the related functions. The SFR FDP_RIP.1/PINPUK requires erasing the temporal values PIN and PUK.

OT.Data_Int (Integrity of personal data) requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM and FDP_ACF.1.4/TRM2). FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE, and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions. Unauthorised modifying of the exchanged data is addressed, in the first line, by FDP_UCT.1/TRM, FDP_UIT.1/TRM, FTP_ITC.1/PACE and FTP_ITC.1/CA2 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 resp. FIA_UAU.6/CA. The trusted channel is established using PACE, Chip Authentication 1 or 2, and Terminal Authentication 1 or 2. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).

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

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

The SFR FCS_COP.1/SHA and FCS_RND.1 represents a general support for cryptographic operations needed.

For SCP03, the SFR FCS_COP.1/GPSCP_MAC ensure the integrity of the data transferred over a dedicated Secure Channel after successful authentication of the authorized user according to FIA_UID.1/GPSCP, FIA_UAU.1/GPSCP, FCS_CKM.1/GPSCP and FCS_COP.1/GPSCP_AUTH.

To allow for a verification of the certificate chain as required in **FMT_MTD.3**, the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as required by **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD** and **FMT_MTD.1/DATE**.Additionally, in the case of eDigitalIdentity configuration, the security objective **OT.Data_Int** is achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA_API.1/CA. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_ PIN support the achievement of these objectives. The SFR FMT_SMF.1/PINPUK support the related functions. The SFR FDP_RIP.1/PINPUK requires erasing the temporal values PIN and PUK.

OT.Data_Conf (Confidentiality of personal data) aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE,

FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KENC). 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 SOD 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.

For SCP03, the SFR FCS_COP.1/GPSCP_ENC ensure the confidentiality of the data transferred over a dedicated Secure Channel after successful authentication of the authorized user according to FIA_UID.1/GPSCP, FIA_UAU.1/GPSCP, FCS_CKM.1/GPSCP and FCS_COP.1/GPSCP_AUTH.

Additionally, in the case of eDigitalIdentity configuration, the security objective **OT.Data_Conf** is achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA_API.1/CA. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_ PIN support the achievement of these objectives. The SFR FMT_SMF.1/PINPUK support the related functions. The SFR FDP_RIP.1/PINPUK requires erasing the temporal values PIN and PUK.

OT.Sense_Data_Conf (Confidentiality of sensitive biometric reference data) is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER. The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE.

The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

The Personalization Agent manages the security environment object data required for Chip Authentication and for Terminal Authentication according to SFR FMT_MTD.1/KEY_WRITE.

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

For SCP03, the SFR FCS_COP.1/GPSCP_ENC ensure the confidentiality of the data transferred over a dedicated Secure Channel after successful authentication of the authorized user according to FIA_UID.1/GPSCP, FIA_UAU.1/GPSCP, FCS_CKM.1/GPSCP and FCS_COP.1/GPSCP_AUTH.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1/CAP 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 [6] 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.

OT.Data_Aut (Authenticity of personal data) aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD 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.

For SCP03, the SFR FCS_COP.1/GPSCP_MAC ensure the authenticity of the data transferred over a dedicated Secure Channel after successful authentication of the authorized user according to FIA_UID.1/GPSCP, FIA_UAU.1/GPSCP, FCS_CKM.1/GPSCP and FCS_COP.1/GPSCP_AUTH.

Additionally, in the case of eDigitalIdentity configuration the security objective **OT.Data_Auth** is achieved by establishing a trusted channel via a successful Chip Authentication thanks to the SFR FIA_API.1/CA. Since PACE can use the PIN as the shared secret, using and management of PIN, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_ PIN support the achievement of these objectives. The SFR FMT_SMF.1/PINPUK support the related functions. The SFR FDP_RIP.1/PINPUK requires erasing the temporal values PIN and PUK.

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

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

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

Additionally, in the case of eDigitalIdentity configuration the security objective **OT.Tracing** is achieved while establishing PACE communication using the PIN/PUK by the SFR FIA_AFL.1/PACE.

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

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

OT.Prot_Inf_Leak (Protection against Information Leakage) requires the TOE to protect confidential TSF data stored and/or processed in the MRTD's chip against disclosure

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

OT.Prot_Phys-Tamper (Protection against Physical Tampering) is covered by the SFR FPT_PHP.3.

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 of **OT.Sens_Data_EAC2** aims to explicitly protect sensitive (as opposed to common) user and TSF-Data. This is mainly achieved by enforcing (FDP_UCT.1/TRM and FDP_UIT.1/TRM) the access control SFPs FDP_ACC.1/TRM and FDP_ACF.1/TRM2. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH_PACE. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/PACE, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Unblock_PIN2 FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Activate_PIN) also support to achieve this objective. FDP_RIP.1/PINPUK requires erasing the temporal values of the PIN and PUK.

FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE and FCS_CKM.4 represent some specific properties of the used protocols. To allow for a verification of the certificate chain as required 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 required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. This objective for the data exchanged is mainly achieved by FTP_ITC.1/CA2 and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CAP2 using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, and FIA_UAU.6/CA. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/PACE, FIA_UAU.1/PACE and FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE.

CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/CAPK governs creating/loading SKPICC C, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus, its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and session keys, here for KENC. FMT_MTD.1/PA requires that only the personalization agent is allowed to modify the SOCC (containing amongst other, the signature of PKPICC) used for Passive Authentication. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles.

The security objective **OT.CA2** aims at enabling verification of the authenticity of the TOE as a whole device. This objective is mainly achieved by FIA_API.1/CAP2 using FCS_CKM.1/DH_PACE. CA2 provides an evidence of possessing the Chip Authentication Private Key (SKPICC). FMT_MTD.1/CAPK governs creating/loading SKPICC, whereas FMT_MTD.1/KEY_READ requires making this key unreadable by

users. Hence, its value remains confidential. FDP_RIP.1 requires erasing the values of SKPICC and the session keys, here for CMAC. The authentication token TPICC is calculated using FCS_COP.1/PACE_MAC. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations.FMT_MTD.1/PA requires that the SOC (containing amongst other, the signature of PKPICC) used for Passive Authentication is allowed to be modified only by the personalization agent only. Hence is to consider as trustworthy.

The security objective **OT.AC_Pers_EAC2** ensures that only the personalization agent can write user- and TSF-Data into the TOE, and that some of this data cannot be altered after personalization. This property is covered by FDP_ACC.1/TRM and FDP_ACF.1/TRM requiring, amongst other, an appropriate authorization level of an EAC2 terminal. This authorization level can be achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the related functions and roles. Since only an EAC2 terminal can reach the necessary authorization level, using and managing the PIN (the related SFRs are FIA_AFL.1/PACE, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Unblock_PIN2 and FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PINPUK) also support the achievement of this objective. FDP_RIP.1 requires erasing the temporal values PIN and PUK. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the pre-personalization data. FMT_MTD.1/PA covers the related property of OT.AC_Pers_EAC2 (writing/updating SOC and SOD and, in generally, personalization data). Updating such data can only be done by the personalization agent prior to the operational phase. Thus, such data cannot be changed after the personalization of the document, as required by OT.AC_Pers_EAC2. Finally, FMT_MTD.1/KEY_READ ensures that cryptographic keys for EAC2 cannot be read by users.

Additional rationale only relevant for configuration “eDigitalIdentity” configuration

The following rationale is only relevant for configuration “eDigitalIdentity”:

OT.Sens_Ident_User_Data_Conf (Confidentiality of sensitive identification user data) aims to explicitly protect sensitive identification user and TSF-Data during their exchange. It is enforcing by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER 1. A prerequisite for establishing a trusted channel is a successful Chip Authentication thanks to the SFRs FIA_API.1/CA. Since PACE can use the PIN as the shared secret, the SFRs FIA_AFL.1/PACE, FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_ PIN support the achievement of this objective. The SFR FMT_SMF.1/PINPUK support the related functions. The SFR FDP_RIP.1/PINPUK requires erasing the temporal values PIN and PUK.

OT.CASS_Replacement (Replacement of Chip Authentication Security Service) is covered by FMT_SMF.1/CASS, FMT_MOF.1/CASS, FMT_MTD.1/CASS ensuring that the TOE supports replacement of Chip Authentication Security Service on demand of the authorized user on behalf of the Issuer.

FDP_RIP.1/CASS ensures that the replaced CASS is made unavailable after replacement operation, and FDP_MTD.1/KEY_WRITE ensures that the replacement and the replaced Chip Authentication Private Key cannot be read before or after the replacement operation.

FPT_FLS.1/CASS will ensure that the TOE stays in a safe state in case the replacement operation fails.

The proper access right to the file system (needed for CASS replacement) and secure channel are managed by FMT_SMR.1/PACE, FIA_UID.1/PACE, FIA_UAU.1/PACE, FCS_CKM.1/DH_PACE, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC.

The GP SCP03 (which is the other way to get the permission of CASS) is modeled by FMT_SMR.1/PACE, FIA_UID.1/GPSCP, FIA_UAU.1/GPSCP, FCS_CKM.1/GPSCP, FCS_COP.1/GPSCP_AUTH, FCS_CKM.1/GPSCP_ENC, FCS_COP.1/GPSCP_MAC.

6.3.3 SFR Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_SAS.1	No dependencies
FCS_CKM.1/CA	FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC and FCS_CKM.4
FCS_CKM.1/DH_PACE	A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4
FCS_CKM.1/KP	FCS_COP.1/SIG_GEN, FCS_CKM.4
FCS_CKM.1/GPSCP	**FCS_COP.1/GPSCP_AUTH, FCS_COP.1/GPSCP_ENC, FCS_COP.1/GPSCP_MAC**, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1/DH_PACE, FCS_CKM.1/KP, FCS_CKM.1/CA, FCS_CKM.1/GPSCP
FCS_COP.1/CA_ENC	FCS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/CA_MAC	FCS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/SIG_VER	FCS_CKM.1/CA and FCS_CKM.4
FCS_COP.1/SIG_GEN	FCS_CKM.1/KP, FCS_CKM.4 and FCS_CKM.1/CA
FCS_COP.1/SHA	The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore, neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary., FCS_CKM.4
FCS_COP.1/PACE_ENC	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/PACE_MAC	FCS_CKM.1/DH_PACE, FCS_CKM.4
FCS_COP.1/GPSCP_AUTH	**FCS_CKM.1/GPSCP**, FCS_CKM.4
FCS_COP.1/GPSCP_ENC	**FCS_CKM.1/GPSCP**, FCS_CKM.4
FCS_COP.1/GPSCP_MAC	**FCS_CKM.1/GPSCP**, FCS_CKM.4
FCS_RND.1	No dependencies
FIA_AFL.1/PACE	FIA_UAU.1/PACE

FIA_UID.1/GPSCP	No dependencies
FIA_UAU.1/GPSCP	**FIA_UID.1/GPSCP**
FIA_UID.1/PACE	No dependencies
FIA_UAU.1/PACE	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies
FIA_UAU.5/PACE	No dependencies
FIA_UAU.6/EAC	No dependencies
FIA_UAU.6/CA	No dependencies
FIA_UAU.6/PACE	No dependencies
FIA_API.1/CAP	No dependencies
FIA_API.1/CAP2	No dependencies
FIA_API.1/AAP	No dependencies
FIA_API.1/CA	No dependencies
FDP_ACC.1/TRM	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1/TRM
FDP_ACF.1/TRM2	FDP_ACC.1/TRM
FDP_RIP.1	No dependencies
FDP_RIP.1/PINPUK	No dependencies
FDP_RIP.1/CASS	No dependencies
FDP_UCT.1/TRM	FTP_ITC.1/PACE and FDP_ACC.1/TRM
FDP_UIT.1/TRM	FTP_ITC.1/PACE and FDP_ACC.1/TRM
FMT_SMF.1	No dependencies
FMT_SMF.1/PINPUK	No dependencies
FMT_SMF.1/CASS	No dependentcies
FMT_SMR.1/PACE	FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2
FTM_LIM.2	FMT_LIM.1
FMT_MOF.1/CASS	FMT_SMF.1/CASS and FMT_SMR.1/PACE
FMT_MTD.1/INI_ENA	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/CASS	FMT_SMF.1/CASS and FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/Initialize_PINPUK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/Resume_PINPUK	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/Change_PIN	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/Unblock_PIN	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.1/Unblock_PIN2	FMT_SMF.1 and FMT_SMR.1/PACE

FMT_MTD.1/Activate_PIN	FMT_SMF.1 and FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1/ CVCA_INI, FMT_MTD.1/ CVCA_UPD
FPT_EMSEC.1	No dependencies
FPT_FLS.1	No dependencies
FPT_FLS.1/CASS	No dependencies
FPT_PHP.3	No dependencies
FPT_TST.1	No dependencies
FTP_ITC.1/PACE	No dependencies
FPT_ITC.1/CA2	No dependencies

Table 10. SFR Dependencies

7. TOE summary specification

This set of TSFs manages the identification and/or authentication of the external user and enforces role separation (FMT_SMR.1).

7.1 SF.Access Control

This function checks that for each operation initiated by a user, the security attributes for user authorization and data communication required are satisfied.

7.2 SF.Card Personalization

This TSF provides MRTD's chip personalization functions to allow the Personalization Agent to create and set the initial MRTD's LDS data.

7.3 SF.Personalizer Authentication

The Personalization Agent is required to be authenticated by the TOE.

7.4 SF.PACE

The Basic Access System and the travel document mutually authenticate by means of a Basic Access Control mechanism, where after the PACE-enabled Basic Access System and the travel document mutually authenticate by means of a PACE v2 protocol.

7.5 SF.Chip Authentication

This TSF provides the Chip Authentication protocol 1 and 2 to allow the Extended Inspection System to authenticate the TOE.

7.6 SF.Terminal Authentication

This TSF provides Terminal Authentication 1 and 2 to allow the TOE to authenticate the terminal using the public authentication material that is presented during the Chip Authentication protocol 1 or PACE (DH or ECDH), enforcing the Secure Messaging session.

7.7 SF.Active Authentication

Active Authentication is provided by this TSF based on the availability of DG15 in the MRTD's chip information data.

7.8 SF.Secure Messaging

Commands and responses are exchanged between the TOE and the external device.

This TSF provides a secure mean for the terminal and the card to exchange data.

7.9 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing.

7.10 SF.Protection

This Security Function is responsible for protection of the TSF data, user data, and TSF functionality.

7.11 SF.Secure Personalization Management

For Secure Pre-Personalization, Secure Personalization, or Secure Platform management, the TSF provides the capability to set-up a dedicated Secure Channel SCP03.

7.12 SF.Chip Authentication Security Service Replacement

This TSF provides the capability to replace the Chip Authentication 1 and 2 Security Service in the field.

8. Additional Rationale

8.1 SAR Dependencies Rationale

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Requirement	Dependencies
ADV_ARC.1	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	ADV_TDS.4, ADV_IMP.1
ADV_IMP.1	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	ADV_FSP.5
AGD_OPE.1	ADV_FSP.5
AGD_PRE.1	No dependencies
ALC_CMC.4	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies
ALC_DEL.1	No dependencies
ALC_DVS.2	No dependencies
ALC_LCD.1	No dependencies
ALC_TAT.2	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies
ASE_TSS.1	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	ATE_COV.2
ATE_IND.2	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

Table 11. SAR Dependencies

8.2 Rationale for Extensions

Extensions are based on the Protection Profile [5] and have all been adopted by the developer of the TOE:

- FAU_SAS.1 ‘Audit data storage’
- FCS_RND.1 ‘Generation of random numbers’
- FIA_API.1 ‘Authentication Proof of Identity’

- FPT_EMSEC.1 ‘TOE emanation’
- FMT_LIM.1 and FMT_LIM.2 ‘limited capability and availability’

8.3 Assurance Measures Rationale

Each assurance requirement is covered by an assurance measure.

Assurance Requirements / Assurance Measures	AM_ADV	AM_AGD	AM_ALC	AM_ATE	AM_AVA
ADV	X				
AGD		X			
ALC			X		
ATE				X	
AVA					X

Table 12. Mapping Assurance Requirements to Assurance Measures

8.4 PP Claim Rationale

This ST includes all the security objectives and requirements claimed by PPs [5] and [6], and, all of the operations applied to the SFRs are in accordance with the requirements of this PP.

8.4.1 PP compliancy

The TOE type is compliant with the claimed PPs: the TOE is an ICAO MRTD’s chip providing all means of identification and authentication of the TOE itself, the MRTD’s traveler and possibly the Terminal.

The TOE is compliant with the representation provided in the ICAO Machine Readable Travel Document Chip with Extended Access Control PP [5] and PACE PP [6].

The compliance is strict: the addition of specific TOE security mechanisms to the security principles of this Security Target required only the addition of three TOE Objectives related to Active Authentication, and eDigitalIdentity needs.

These additions do not affect the concept defined in the PP [5] and this ST is a suitable solution to the generic security problem described in the PP.

9. Terminology

Term	Definition
Active Authentication	Security mechanism defined in [11] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined in [11] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [11]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
CAN (Card Access Number)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [11]
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.

Term	Definition
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [11], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric (two-key) TDES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [11]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [11]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [11]
Extended Access Control	Security mechanism identified in [11] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Term	Definition
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [11]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [11]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [11]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [11]
Initialization	Process of writing Initialization Data (see below) to the TOE (cf. 1.3.9.2 TOE lifecycle phase 2 step 3).
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [11]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

Term	Definition
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [11]
Issuing State	The Country issuing the MRTD. [11]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [11]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [11] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to): (1) personal data of the MRTD holder, (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16, EF.COM, EF.SOD, EF.CardAcces, EF.CardSecurity)
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [11]
Machine readable visa (MRV)	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [11]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [11]

Term	Definition
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [11]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes the file structure implementing the LDS [11], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [3]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment" (cf. 1.3.9.3, TOE lifecycle phase 3 step 6).

Term	Definition
Personalization Agent	The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent.
Physical travel Document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and other data
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the MRTD Application (cf. 1.3.9.2, TOE lifecycle phase 2 step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between lifecycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.
Receiving State	The Country to which the Traveler is applying for entry. [11]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [11]
Secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 Skimming Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

Term	Definition
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel.
Traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
Un-personalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [11]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

10. References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[4] BSI-CC-PP0055 – Protection Profile - Machine Readable Travel Document with “ICAO Application”, Basic Access Control – EAL 4+ – Version: 1.10, 25th March 2009

[5] BSI-CC-PP-0056-V2-2012 – Protection Profile - Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP) – EAL 4+ – Version: 1.3.2, 05th December 2012

[6] BSI-CC-PP0068-V2-2011-MA-01 – Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP) – EAL 4+ – Version: 1.01, 22nd July 2014

[7] PKCS#1: RSA Cryptography Standard, Version 1.5

[8] Specifications for the Java Card 3 Platform, Version 3.0.4 Classic Edition, Sept. 2011
- Virtual Machine Specification [JCVM]
- Application Programming Interface [JCAPI]
- Runtime Environment Specification [JCRE]

[9] - GlobalPlatform, Card Specification, Version 2.3.1, March 2018 [GPC_SPE_034]
- GlobalPlatform Secure Channel Protocol 03 – Amendment D, v1.1.2, March 2019 [GPC_SPE_014]

[10] CCDB-2007-09-001 – Composite product evaluation for Smart Cards and similar devices – Version: 1.0, revision 1, September 2007

[11] ICAO Doc 9303, Machine Readable Travel Documents, , Seventh Edition, 2015, International Civil Aviation Organization

[12] TR-03110-1, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015, BSI

[13] TR-03110-2, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic Identification, Authentication and trust Services (eIDES), Version 2.21, 21 December 2016, BSI

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

[15] ICAO: Supplement to doc 9303 – Release 11 – November 17, 2011

[16] ICAO: Technical report supplemental access control for machine readable travel documents – Version 1.01 – November 11, 2010

[17] TR-03111, Technical Guideline Elliptic Curve Cryptography, Version 2.0, 28 June 2012, BSI

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

[19] ISO/IEC 9796-2: Information technology — Security techniques — Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms, 2002

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

[21] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[22] FIPS PUB 180-2, FIPS Publication – Secure hash standard (+ Change Notice to include SHA-224), 2002, NIST

[23] FIPS PUB 46-3, FIPS Publication – Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department of Commerce/NIST

[24] IEEE 1363-2000 – IEEE Standard Specification for Public-Key Cryptography

[25] ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999

[26] NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB 197-2001

[27] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, special publication 800-38B-2005

[28] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3), Security Target Lite, NXP Semiconductors, Rev. 2.5, 4 May 2022, , BSI-DSZ-CC-1136-V2-2022

[29] JCOP 4 P71 Security Target Lite for JCOP 4 P71 / SE050, NXP Semiconductors, Rev. 4.5, 10 June 2022, NSCIB CC-22-180212

[30] ChipDoc 3.1 User Guide Manual, Ref. 518830, Revision 3.0, Date: 17 August 2020

[31] ChipDoc 3.1 ICAO Personalization Guide, Ref. 518933, Revision: 3.3, Date: 17 December 2020

[32] ChipDoc 3.1 Crypto Guide, Ref. CDv3.1_2_03210_ChipDoc3.1_Crypto-Guide, Revision: 1.0, Date: 4 December 2020

[33] ChipDoc V3 Application note, Revision: 1.4, Date: 20 June 2022

[34] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

[35] BSI: TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents. Part 2 - Extended Access Control Version 2 (EACv2), Password

Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.10, 20. March 2012

[36] Common Criteria Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, BSI-CC-PP-0086, Version 1.01, May 20th, 2015, BSI

[37] Module: Annexe PP0056v2 eDigitalIdentity document using Remote Access Control with PACE v2, v1.1, 21 November 2019

[38] Electronic National Identity Card Technical Specifications, Version A028, Date: 24/03/2020

[39] BSI-CC-PP-0086 – Common Criteria Protection Profile – Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 [EAC2-PP], Version: 1.01, May 20th 2015

[40] BSI-CC-PP-0087 – Common Criteria Protection Profile – Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], Version: 2.0.3, July 18th 2016

11. Legal information

11.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

11.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

11.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

12. List of figures

Fig 1. Components of the TOE 3
Fig 2. TOE Life Cycle.....12
Fig 3. Remote Inspection Procedure.....23

13. List of tables

Table 1. ST Reference and TOE Reference 3
Table 2. Reference to Certified Micro Controller with IC Dedicated Software and Crypto Library 9
Table 3. Reference to certified Platform 10
Table 4. ChipDoc v3.1 P71 configurations and identification 11
Table 5. Terminology synonyms for the configurations 11
Table 6. Delivery Items 14
Table 7. Security Environment to Security Objectives Mapping 40
Table 8. Assurance Requirements: EAL5 augmented 90
Table 9. Functional Requirement to TOE Security Objective Mapping 94
Table 10. SFR Dependencies 104
Table 11. SAR Dependencies 107
Table 12. Mapping Assurance Requirements to Assurance Measures 108

14. Contents

1. ST Introduction (ASE_INT) 3
1.1 ST Reference and TOE Reference 3
1.2 TOE Overview 3
1.2.1 TOE Usage and Security Features for Operational Use 4
1.3 TOE Description 5
1.3.1 General 5
1.3.2 MRTD's Chip 6
1.3.3 Basic Access Control 6
1.3.4 PACE 7
1.3.5 Extended Access Control 1 8
1.3.6 Extended Access Control 2 8
1.3.7 Active Authentication 9
1.3.8 TOE Components and Composite Certification 9
1.3.8.1 Micro Controller 9
1.3.8.2 Security IC Dedicated Software 9
1.3.8.3 Security IC Embedded Software 10
1.3.9 TOE Lifecycle 11
1.3.9.1 Phase 1 "Development" 11
1.3.9.2 Phase 2 "Manufacturing" 12
1.3.9.3 Phase 3 "Personalization of the MRTD" 13
1.3.9.4 Phase 4 "Operational Use" 14
1.3.10 TOE Identification 14
1.3.10.1 TOE Delivery 14
1.3.10.2 Identification of the TOE 14
1.3.11 Evaluated Package Types 15
2. Conformance Claims 16
2.1 CC Conformance Claim 16
2.2 Package Claim 16
2.3 PP Claim 16
3. Security Problem Definition 18
3.1 Assets 18
3.1.1 ICAO assets 18
3.1.2 Refinements relevant for configuration "eDigitialIdentity" 19
3.1.2.1 Primary Assets 19
3.1.2.2 Secondary Assets 20
3.2 Subjects 20
3.2.1 Refinements relevant for configuration "eDigitialIdentity" 22
3.3 Assumptions 23
3.4 Threat agent 24
3.5 Threats 25
3.5.1 Additional Threat relevant for configuration "eDigitialIdentity" 27
3.6 Organisational Security Policies 27
3.6.1 Additional OSP relevant for configuration "eDigitialIdentity" 30
4. Security Objectives 31
4.1 SOs for the TOE 31
4.1.1 Additional SOs relevant for configuration "eDigitialIdentity" 35
4.2 Objective on the Environment 36
4.2.1 Additional OEs relevant for configuration "eDigitialIdentity" 39
4.3 Security objectives rationale 39
4.3.1 Security Objectives Coverage 39
4.3.2 Security Objectives Sufficiency 40
4.3.2.1 Additional Security Objectives Sufficiency relevant for configuration "eDigitalIdentity" 44
5. Extended Components Definition 46
5.1 Audit data storage (FAU_SAS) 46
5.2 Generation of random numbers (FCS_RND) 47
5.3 Authentication Proof of Identity (FIA_API) 48
5.4 Limited capabilities and availability (FMT_LIM) 49
5.5 TOE emanation (FPT_EMSEC.1) 51
6. Security Requirements 52
6.1 TOE Security Functional Requirements 56
6.1.1 Security Audit (FAU) 56
6.1.1.1 Audit Storage (FAU_SAS.1) 56
6.1.2 Cryptographic support (FCS) 56
6.1.2.1 Cryptographic key generation (FCS_CKM.1) 57

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 13 July 2022
Document identifier: CDv3.1_2_31339_STLite_CDv3.1_ICAO_EAC_PACE

6.1.2.2 Cryptographic key destruction (FCS_CKM.4) ..58
6.1.2.3 Cryptographic operation (FCS_COP.1).....58
6.1.2.4 Random Number Generation (FCS_RND.1)....61
6.1.3 Identification and authentication (FIA).....62
6.1.3.1 Authentication Failure Handling (FIA_AFL.1)...62
6.1.3.2 Timing of identification (FIA_UID.1) 64
6.1.3.3 Timing of authentication (FIA_UAU.1).....65
6.1.3.4 Single-use authentication mechanisms (FIA_UAU.4).....66
6.1.3.5 Multiple authentication mechanisms (FIA_UAU.5).....67
6.1.3.6 Re-authenticating (FIA_UAU.6).....69
6.1.3.7 Authentication Proof of Identity (FIA_API.1).....69
6.1.4 User data protection (FDP) 70
6.1.4.1 Subset access control (FDP_ACC.1) 70
6.1.4.2 Security attribute based access control (FDP_ACF.1) 71
6.1.4.3 Residual Information Protection (FDP_RIP.1)..77
6.1.4.4 Basic data exchange confidentiality (FDP_UCT.1) 78
6.1.4.5 Data exchange integrity (FDP_UIT.1) 78
6.1.5 Security Management (FMT).....78
6.1.5.1 Specifications of Management Functions (FMT_SMF.1).....78
6.1.5.2 Security roles (FMT_SMR.1).....79
6.1.5.3 Limited capabilities (FMT_LIM.1) 80
6.1.5.4 Limited availability (FMT_LIM.2) 80
6.1.5.5 Additional SFRs relevant for “eDigitalIdentity”: Management of security functions behavior (FMT_MOF.1) 80
6.1.5.6 Management of TSF data (FMT_MTD.1).....81
6.1.5.7 Secure TSF data (FMT_MTD.3).....85
6.1.6 Protection of the TSF (FPT) 86
6.1.6.1 TOE Emanation (FPT_EMSEC.1).....86
6.1.6.2 Failure with preservation of secure state (FPT_FLS.1) 87
6.1.6.3 Resistance to physical attack (FPT_PHP.3).....88
6.1.6.4 TSF testing (FPT_TST.1).....88
6.1.7 Trusted Path/Channels (FTP) 88
6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1).....88
6.2 TOE Security Assurance Requirements.....90
6.2.1 SARs Measures 90
6.2.2 SARs Rationale 91
6.3 Security Requirements Rationale 92
6.3.1 Security Requirement Coverage 92
6.3.2 Security Requirements Sufficiency.....94
6.3.2.1 TOE Security Requirements Sufficiency 94
6.3.3 SFR Dependencies 102
7. TOE summary specification 105
7.1 SF.Access Control.....105
7.2 SF.Card Personalization.....105
7.3 SF.Personalizer Authentication 105
7.4 SF.PACE.....105
7.5 SF.Chip Authentication.....105
7.6 SF.Terminal Authentication 105
7.7 SF.Active Authentication 105
7.8 SF.Secure Messaging 105
7.9 SF.Crypto 105
7.10 SF.Protection.....106
7.11 SF.Secure Personalization Management 106
7.12 SF.Chip Authentication Security Service Replacement 106
8. Additional Rationale.....107
8.1 SAR Dependencies Rationale 107
8.2 Rationale for Extensions.....107
8.3 Assurance Measures Rationale.....108
8.4 PP Claim Rationale 108
8.4.1 PP compliancy.....108
9. Terminology.....109
10. References.....116
11. Legal information 119
11.1 Definitions.....119
11.2 Disclaimers.....119
11.3 Trademarks 119
12. List of figures.....120
13. List of tables 121
14. Contents.....122

For more information, visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 13 July 2022
Document identifier: CDv3.1_2_31339_STLite_CDv3.1_ICAO_EAC_PACE