ChipDoc v4 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration

Security Target Lite

Rev. 9.0 — 24 January 2023

Evaluation document

Document information

Information	Content
Keywords	Common Criteria, Security Target Lite, ChipDoc v4, JCOP 4.5 P71, ICAO EAC with BAC, ICAO EAC with PACE
Abstract	Security Target Lite of ChipDoc v4 application on JCOP 4.5 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
5.0	20 October 2022	First release (Revision aligned with ST).
6.0	24 November 2022	Updated Applet version in Table 2 and Table 5, updated user manual in Table 5 and Chapter 9.
7.9	12 January 2023	Update IC and Platform certification references
8.0	18 January 2023	Corrected statement in chapter 2.2 about PP0056v2 Annex Module for eDigitalIdentity
9.0	24 January 2023	Updated UGM revision in Table 5 and Chapter 9. Updated revision of ETSI TS 119312 in Chapter 9.

Acronyms

AA - Active Authentication

ADF - Application Dedicated File

AID - Applet IDentifier

BAC - Basic Access Control

BIS-PACE - Basic Inspection System with PACE protocol

CA - Certification Authority

CAN - Card Access Number

CASS - Chip Authentication Security Service

CC - Common Criteria

CGA - Certificate Generation Application

CSP - Certification Service Provider

CSCA - Country Signing Certification Authority

CVCA - Country Verifying Certification Authority

DG - Data Group

DH - Diffie-Hellman

DTBS - Data To Be Signed

DTBS/R - Data To Be Signed or its Representation

DS - Document Signer

DV - Document Verifyer

EAC - Extended Access Control

EAL - Evaluation Assurance Level

EIS - Extended Inspection System

ECC - Elliptic Curve Cryptography

ECDH - Elliptic-curves Diffie-Hellman

EF - Elementary File

eDL- electronic Driving Licence

eID - electronic IDentity

eIDAS - electronic IDentification, Authentication and trust Services

ePP - electronic PassPort

eTD - electronic Travel Document

FID - File IDentifier

FW - FirmWare

GP - GlobalPlatfom®

HID - Human Interface Device

IC - Intregrated Circuit

ICAO - International Civil Aviation Organization

IS - Inspection System

ISD - Issuer Security Domain

JC - Java Card

JCAPI - Java Card API

JCRE - Java Card Runtime Environment

JCVM - Java Card Virtual Machine

LDS - Logical Data Structure

MC - MicroControler

MF - Master File

MRTD - Machine Readable Travel Document

MRZ - Machine Readable Zone

NVM - Non-Volatile Memory

OS - Operating System

OSP - Organizational Security Policy

PA - Personalization Agent

PACE - Password Authenticated Connection Establishment

PACE-GM - PACE General Mapping

PACE-IM - PACE Integrated Mapping

PACE-CAM - PACE Chip Authentication Mapping

PIN - Personal Identification Number

PKI - Public Key Infrastructure

PP - Protection Profile

PUF - Physically Unclonable Function

PUF-EPP - PUF Enhanced Privacy Protection

PUK - PIN Unlock Key

QSCD - Qualified Signature Creation Device

RAD -Reference Authentication Data

ROM - Read-Only Memory

SCA - Signature Creation Application

SCD - Signature Creation Data

SCP - Secure Channel Protocol

SDO - Security Data Object

SFR - Security Functional Requirement

SSCD - Secure Signature Creation Device

ST - Security Target

SVD - Signature Creation Data

TA - Terminal Authentication

TOE - Target Of Evaluation

TSF - TOE Security Functionality

VAD - Verification Authentication Data

1 ST Introduction

1.1 Introduction

NXP ChipDoc v4 Java Card application offers identification, authentication, and secure signature functionalities allowing a variety of configurations like electronic identification (eID), electronic passport (ePP), or secured signature creation device (SSCD).

This document is the Security Target for the Common Criteria composite evaluation of the NXP ChipDoc v4 Java Card application in its ICAO EAC(1&2) with PACE configuration, loaded onto the NXP JCOP 4.5 P71 Platform.

1.2 ST Reference

Table 1. ST Reference

ST Title	ChipDoc v4 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration Security Target Lite
ST Reference	CDv4_1_310390_STLite_CDv4_ICAO_EAC_PACE
ST Version	Version 9.0
ST Date	24 January 2022

1.3 TOE Reference

Table 2. TOE Reference

TOE Name	ChipDoc v4 on JCOP 4.5 P71 in ICAO EAC(1&2) with PACE configuration Lite[1]
Applet Version	4.0.1.52
Applet Identification[2]	Name (ASCII) : 43686970446F63 Version : 04000152 Card capabilities : 0003EFEF

[1] Applet configuration can be verified as described in section "2.3 Applet configuration" of the Personalization Guidance for this TOE [14]

[2] Applet identification can be verified using GET_DATA command according the instructions in section "2.2 Applet Identification" of the Personalization Guidance for this TOE [14]

Table 3. Platform Reference

Platform Name	JCOP 4.5 P71
Platform Identification[1]	Platform ID (ASCII) : 4A335236303030333733313831323030 ROM ID : B3375FE9B5508BC4 Build ID : 6D20B6197D635E7C OS Core : 55606FD4BEECF3CD Patch ID : 0000000000000000
Platform Certificate and ST	NSCIB CC-22-0313985 [17]

[1] Platform identification can be verified using GET_DATA(IDENTIFY) command according the instructions in section "2.2 Platform Identification" of the Personalization Guidance for this TOE [14]

Table 4. IC Reference

IC name	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library
IC Certificate and ST	BSI-DSZ-CC-1149-2022 [16]

The ICAO EAC(1&2) with PACE configuration with PACE can be identifed by checking the presence of the EF.CardAccess file (which should contain the OIDs of the required PACE passwords) and the presence of the EF.DG14. For more details see instructions in section "2.3 Applet configuration" of the Personalization Guidance for this TOE [14]).

1.4 TOE Overview

The TOE is the ChipDoc v4 Java Card applet in ICAO EAC(1&2) with PACE configuration installed on the JCOP 4.5 P71 Java Card platform and the N7122 Micro Controller. The TOE is evaluated according to the composition approach as described in [5]. Details about each component of the TOE can be found in Section 1.5.1.

The TOE implements a Machine Readable Travel Document (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and within the framework provided by the Protection Profiles referenced in Section 2.2.

The TOE implements cryptographic mechanisms that are compliant to the ETSI TS 119312 [19] when mandatory recommendations provided in the Guidance Documentation are applied (see TOE Delivery in Section 1.5.2).

As a contact / contactless electronic document compliant with the TR03110-1 [28], the TOE protects the user sensitive data (with EAC1), the user common data (with PACE MRZ/CAN), and the TSF data needed to execute the access protocols or to verify the integrity and authenticity of user data. In addition to that, the TOE supports user authentication by (PACE) PIN/PUK, Symetric Key, or Biometry, and also supports additional authentication protocols as defined in TR03110-2 [29] and TR03110-3 [30] allowing both ePP (travel document) or eID (identity document) application types:

- PACE authentication (PACE-GM, PACE-IM, PACE-CAM) with multiple PIN, PUK, MRZ, or CAN
- Extended Acces Control v1 (EAC1) with Chip Authentication v1 (CA1) and Terminal Authentication v1 (TA1)
- Extended Acces Control v2 (EAC2) with Chip Authentication v2 (CA2) and Terminal Authentication v2 (TA2)

The TOE also supports the Basic Access Control mechanism (BAC) for interoperability reasons. Nevertherless the BAC mechanism **is not included in the scope of TOE** due to a lower resistance level. The BAC functionality is covered through a dedicated Security Target that complies with the BAC PP0055 [10].

The TOE type is compliant with the TOE type defined in the Protection Profile(s) referenced in Section 2.2, to which the current ST claims strict conformance.

For the additional authentication protocols (PACE PIN/PUK, EAC2), dedicated security problem definition, objectives, and SFRs have been imported from the MR.ED-PP (PP0087) [11] and/or the EAC2-PP (PP0086) [7]) without interfering with the ICAO aspects. Those dedicated statements are to be considered only if the corresponding functionalities are configured during personalization of the TOE.

The TOE is delivered in open configuration, meaning that next to the interfaces provided by the ICAO application, GlobalPlatform® (GP) interfaces to load and delete other applications are available.

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

1.5 TOE Description

1.5.1 TOE Components

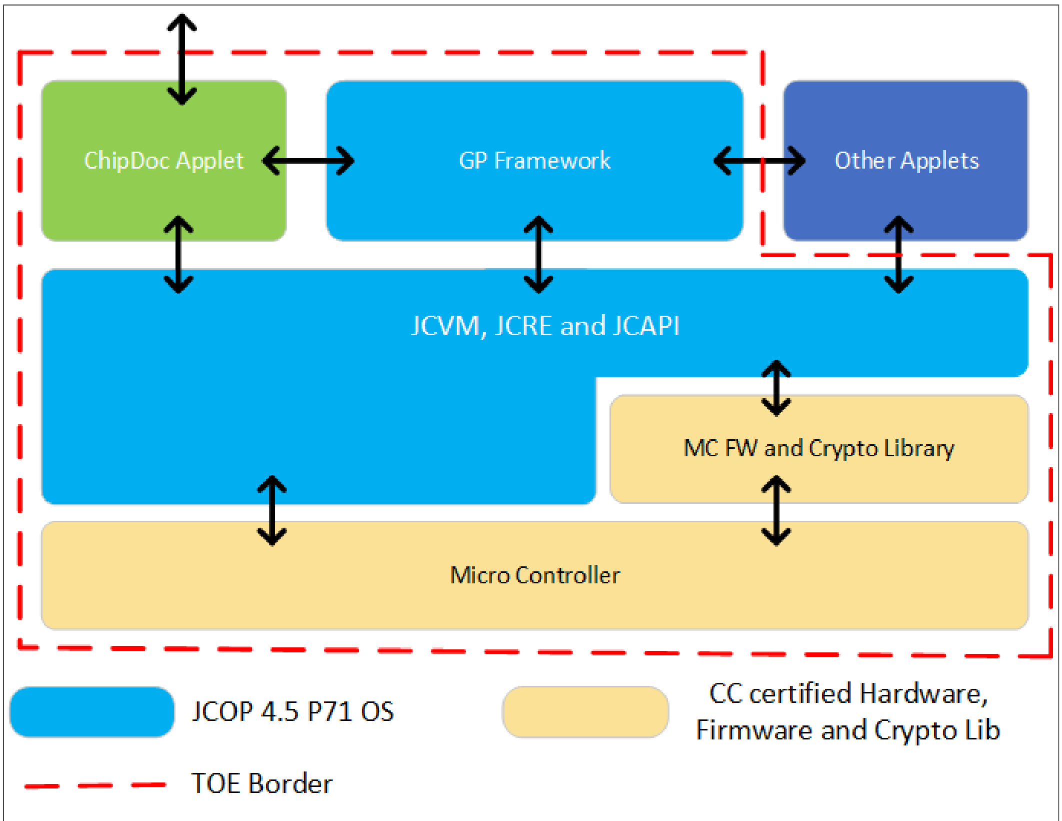

Figure 1. Components of the TOE

The TOE is made of:

- The IC with its IC dedicated Software (Firmware and Cryptographic Library) providing secured execution environment, support for cryptographic operations, and memory management. The IC certificate is re-used for the current evaluation (see the IC Security Target [16] for more details).
- The Java Card Operating System implementing the JCVM, JCRE, JCAPI and the GP framework. The Platform certificate (JC OS + IC) is re-used for the current evaluation (see the Platform Security Target [17] for more details).
- The ChipDoc v4 Applet in ICAO EAC(1&2) with PACE configuration. This functionality is subject of the current certification and thus forms the composite product from formal point of view.
- The TOE Guidance documentation as identified in Section 1.5.2.

1.5.2 TOE Delivery

The TOE delivery comprises the following items:

Table 5. Delivery Items

Type	Name	Version	Form of delivery
JCOP 4.5 P71 Platform	NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library ROM Code (Platform ID) FLASH content (FLASH ID) Patch Code (Patch ID)	JCOP 4.5 P71	Micro Controller including on-chip software: Firmware, Crypto Library and JCOP 4.5 Operating System
ChipDoc v4 Application	FLASH content	4.0.1.52	Application Software loaded onto the IC OR Standelone CAP file encrypted and signed according to GP Amd I [37]
Document	ChipDoc 4.0 User Guide Manual [12]	1.4	Electronic document encrypted and signed
Document	ChipDoc 4.0 Applet Release Note - Release Note for ChipDoc 4.0.1.4JxR Applet [15]	1.1	Electronic document encrypted and signed
Document	ChipDoc 4.0 ICAO Personalization Guide [14]	1.1	Electronic document encrypted and signed

The Platform guidance documents are referenced in the Platform Security Target [17]

1.5.3 Physical scope of the TOE

The physical scope of the TOE is the bare IC loaded with the software components identified in Section 1.5.1 (IC dedicated software, Java Card Operating System, Applet).

The physical interfaces of the TOE are the die surfaces, the ISO7816 communication port (contact) and the ISO14443 communication port (contactless). For contactless operation the TOE needs to be connected with an external antenna which is not part of the TOE.

A number of package types are supported for this TOE. The package types do not influence the security functionality of the TOE. 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.

1.5.4 Logical scope of the TOE

1.5.4.1 ICAO ePP functionalities

The TOE provides access control, strong authentication, and protection of sensitive personal data. The TOE allows:

Access control and secure communication based on PACE authentication

The TOE supports the PACE protocol with

- MRZ or CAN

- DH/ECDH key agreement in Generic, Integrated, or Chip Authentication Mapping

The PACE MRZ/CAN protocol allows granting access to less sensitive user data (by presenting the electronic document) and establishment of a secure channel between the electronic document and the terminal. For ICAO ePP application the PACE MRZ is mandatory and the PACE CAN is optional.

Extended Access Control (EAC) v1

EAC1 provides strong authentication of both electronic document and terminal, with dedicated session keys that protect sensitive personal data.

- Chip Authentication 1 (CA1) authenticates the TOE to the terminal based on a DH/ECDH key exchange protocol and establishes a new secure channel with the terminal.
- Terminal Authentication 1 (TA1) is performed if CA1 has been successfully executed. It authenticates the terminal to the TOE based on certificates verification, and provides an authorized access to sensitive data.

1.5.4.2 Additional Functionalities

User Authentication & try counters

The TOE provides functions to manage the user auhentication data:

- Support for global CVM PIN,
- create, verify, change, unblock the Arbitrary PINs, global CVM PIN, Default PACE PIN, PUKs, Biometric Finger 1:1/1:N or Face Data, Symetric Authentication keys,
- suspend, resume the Default PACE PIN,
- Initialize, delete the Personalization Agen key.

Access control and secure communication based on PACE PIN/PUK

The TOE supports PACE protocol with

- (multiple) PIN, PUK
- DH/ECDH key agreement in Generic, Integrated, or Chip Authentication Mapping
- PIN/PUK suspend mechanism

PACE PIN/PUK is not required for ICAO ePP application but may be required for other ICAO based applications like eID. PACE PIN/PUK may be configured during the Preparation of the TOE (note that PACE CAN is mandatory for suspending PINs/PUKs).

Extended Access Control (EAC) v2

EAC2 provides strong authentication of both electronic document and terminal, with dedicated session keys that protect sensitive personal data.

- Terminal Authentication 2 (TA2) is an authentication of the terminal to the TOE based on certificates verification, and provides the terminal an authorized access to sensitive data.
- Chip Authentication 2 (CA2) is performed if TA2 has been successfully executed. It authenticates the TOE to the terminal based on a DH/ECDH key exchange protocol and establishes a new secure channel with the terminal.

EAC2 may be configured during the Preparation of the TOE.

Active Authentication

The TOE supports the Active Authentication mechanism (AA) as defined in the ICAO DOC 9303 [33] allowing the travel document's chip to prove and the inspection system to verify the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State or Organisation.

Chip Authentication Keys replacement

The TOE provides a specific funtionality that allows replacement of the Chip Authentication keys material in the field. This can be done in two ways:

- by loading new key material using dedicated commands.
- without loading any data by switching the AID, FID and Life cycle state of the current ADF to another replacement ADF that was prepared during the Personalization phase.

This funcitonality requires appropriate access condition to the ADFs or GP-SCP secure channel. This functionality is not expected to be used for ICAO ePP application but only for eID application. The replacement ADF may be prepared and loaded during the Preparation of the TOE.

Functionalities enforced by the Platform

The Platform provides a number of functionalities that are not directly enforced by the ChipDoc v4 applet but for which the applet provides interfaces:

- GP-SCP available from step 5' (pre-personalization) to step 7 (Toe administration during the User phase) of the life-cycle allowing secure (pre-)personalization and secure administration post delivery.
- NXP PUF based Enhanced Privacy Protection (PUF-EPP). When PUF-EPP is enabled for an Elementary File (EF), the data stored in that EF is AES encrypted using a PUF protected AES 256 bit key. By this way, the sensitive user data is not compromised if the NVM of an e-document is somehow cloned and analysed. This option must be selected at the creation of the EF.
- TOE update in the field: The Platform supports GP2.3 Amendment H [36]. ChipDoc v4 application implements the mandatory onSave()/onCleanup() and onRestore() methods needed for its own update in the field.

Other funcitonalities provided by the Platform

- Cryptographic functionalities
- Protection against physical tampering and environmental conditions manipulations
- Self Test and protection against malfunction
- Java Card Security Domains and Bytecode Execution enforcement

The current security target is "maximized" and covers all the additional functionalities needed for PACE PIN/PUK, EAC2, Active Authentication, and Chip Authentication keys replacement. The modular writing of the ST allows any combination of those functionalities as prepared during the personalization phase, by ignoring non-relevent Security Problem Definition, Objectives, and SFRs.

1.6 TOE Life Cycle

The IC Developer, IC Manufacturer as well as the Embedded Software Developer of this TOE is NXP Semiconductors. In particular the software development for this composite TOE took place at “NXP Gratkorn, Mikron-Weg 1, A-8101 Gratkorn, Austria” and the testing took place in “NXP Glasgow, Pegasus House, Scottish Enterprise Technology Park, Bramah Ave, East Kilbride Glasgow, G75 ORD, Scotland United Kingdom" and

"NXP Bangalore, NXP India Private Limited Manyata, Tech Park Nagawara Village, Kasaba Hobli, Bangalore 560045, India". All other sites contributing to the Lifecycle of this TOE can be read from the certification report of the underlying IC[1].

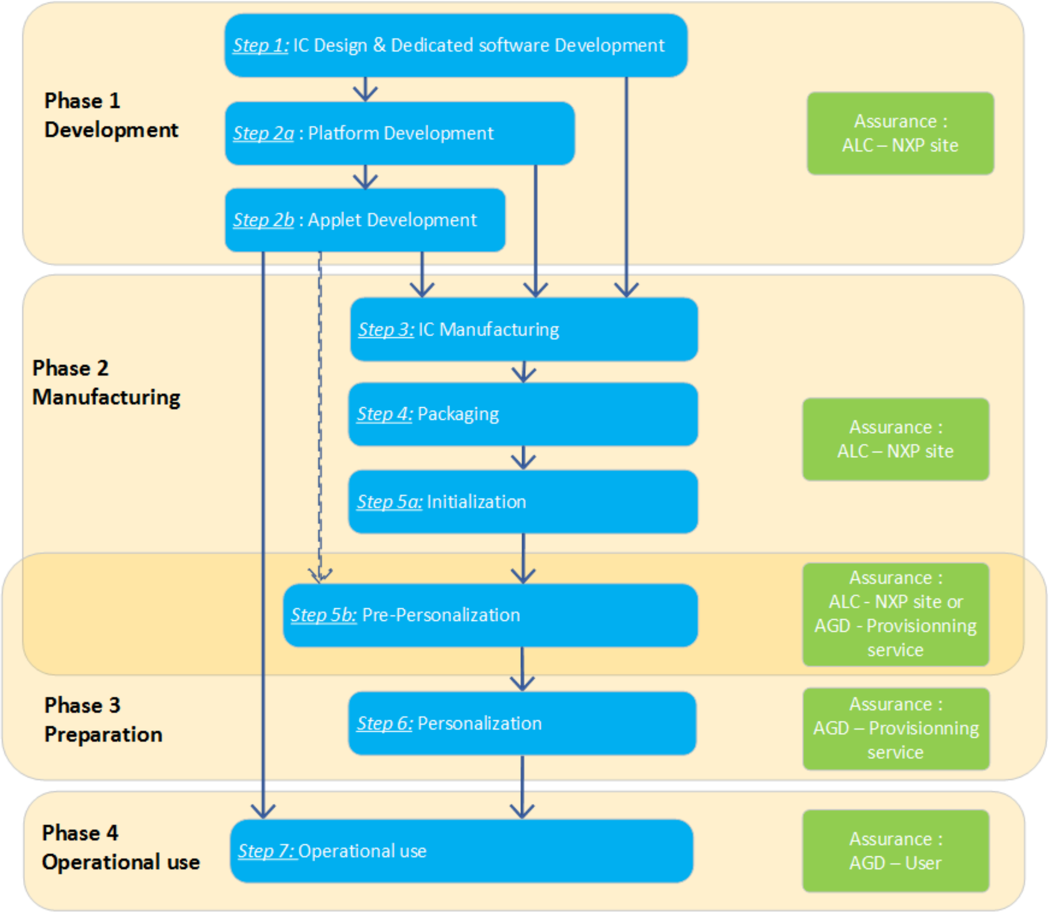
Phase 1
Development
Step 1: IC Design & Dedicated software Development
Step 2a : Platform Development
Step 2b : Applet Development
Assurance : ALC – NXP site
Phase 2
Manufacturing
Step 3: IC Manufacturing
Step 4: Packaging
Step 5a: Initialization
Assurance : ALC – NXP site
Step 5b: Pre-Personalization
Assurance : ALC - NXP site or AGD - Provisionning service
Phase 3
Preparation
Step 6: Personalization
Assurance : AGD – Provisionning service
Phase 4
Operational use
Step 7: Operational use
Assurance : AGD – User

Figure 2. TOE life cycle

Phase1 Development

Step 1: IC design and IC Dedicated Software development (including Guidance documentation) by NXP Semiconductors.

Step 2: Embedded Software development (including Java Card OS, ChipDoc Applet, and Guidance documentation) by NXP Semiconductors.

Phase 2 Manufacturing

Step 3: IC Manufacturing by NXP Semiconductors. The core part of the OS and the IC Dedicated Software are masked into ROM, the modular part of the OS is loaded into Flash, and the TOE is equiped with diversified Transport Key knowledge of which is required for the next steps of the life cycle.

Step 4: IC Packaging. IC is combined with the hardware package, and with contact/ contctless interfaces.

Step 5a: Product initialization by NXP Semiconductors. After authentication with the Transport Key the OS is initialized and configured, the Applet loaded (optional), the

[1] BSI-DSZ-CC-1149-2022

Patches are applied (if any), and the Transport Keys are replaced by ISD keys. The GP state is switched from "Initialized" to "Secured".

Phase 3 Preparation

Step 5b: Product Pre-Personalization by NXP Semiconductors or a Provisionning Service Provider according to the Preparation Documentation [13]. The applet is loaded (if not already pre-loaded), installed (if not already installed), and the MF created (if not already created). At this point a Personalization Agent key can be configured. Pre-Personalization can only be performed under Platform Secure Mode (ISD GP-SCP keys needed).

Step 6: Product Personalization by the Provisioning Service Provider according to the Preparation Documentation [13]. The application ADF is created and the TOE is personalized with:

- survey of the travel document holder’s biographical data,
- enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- personalization of the visual readable data onto the physical part of the travel document,
- writing of the TOE User Data and TSF Data into the logical travel document (digital MRZ data (EF.DG1), (igitized portrait (EF.DG2), and Document security object),
- configuration of the TSF if necessary.

The Personalization steps can be executed in clear (for CC certified environment) or via a GP-SCP "Secure Platform Management" (for non-certified environment) depending on the Security Level configured during the Applet installation (Step5b).

In addition to the certified ICAO file system, other file systems may be configured and coexist inside ChipDoc v4. Moreover, other Applets may be installed beside ChipDoc v4.

Phase 4 User Phase

Step 7: TOE usage according to the Guidance Documentation [12].

During this phase the Chip Authentication keys and associated Data can be updated (for eID application type).

Moreover, ChipDoc v4 itslef can be updated in the field using GP2.3 Amendment H [36] capabilities of the Platform. The current Security Target only covers ChipDoc v4 application version(s) identified in Section 1.3. Any future version of the TOE to be uploaded in the field shall undergo its proper security certification.

In User Phase other applications can also be loaded on JCOP 4.5 P71 platform beside ChipDoc v4.

TOE delivery point(s)

- after *Setp 5a* when the Pre-personalization is handled by the Provisionning Service Provider,
- after *Setp 5b* when the Pre-personalization is handled by NXP Semiconductors,
- after *Setp 2* when ChipDoc v4 Applet package is delivered independently (e.g. for field upgrade).

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims conformance to Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [3].

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017 [4].

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in Section 5.

2.2 PP Claim

This Security Target claims strict conformance to the following Protection Profile(s):

- [EAC-PP-V2] (EAC with PACE configuration) : Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC-PP-V2), certified under the reference BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2 [6].

As the EAC-PP-V2 [6] claims strict conformance to the PACE-PP (BSI-CC-PP-0068-V2-2011-MA-01 [9]), the current Security Target is also strictly compliant with the PACE-PP [9].

Note: The current Security Target is also written in order to match with the PP0056v2 Annex Module for eDigitalIdentity [8]. However, no formal compliance can be claimed as this document is not a certified Protection Profile.

2.3 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

2.4 Conformance Claim Rationale

The conformance claim rationale is given in section Section 8.3

3 Security Problem Definition

3.1 Assets

Assets are strictly compliant with the Assets decribed in the PPs claimed in Section 2.2.

Some Assets have been reworded according to PP0086 [7] and/or PP0087 [11] in order to make them more generic ("travel document" replaced by "electronic document") and to include additional mechanisms (EAC2, eID), without altering the compliance to claimed PPs.

3.1.1 Primary Assets

Authenticity of the Electronic Document's Chip - *(PACE, EAC1, EAC2)*

The authenticity of the electronic document's chip personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document. *(Authenticity)*.

Electronic Document Tracing Data - *(PACE, EAC1, EAC2)*

Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered. *(Unavailability)*.

Sensitive User Data - *(EAC1, EAC2)*

User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC1, EAC2, or both. *(Confidentiality, Integrity, Authenticity)*.

This asset includes:

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

User Data stored on the TOE - *(PACE, EAC1, EAC2)*

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be read out, used or modified either by a PACE terminal, or, in the case of sensitive data, by an EAC1 terminal or an EAC2 terminal with appropriate authorization level. *(Confidentiality, Integrity, Authenticity)*.

This asset includes the "Sensitive User Data" as described separatly, and the "Logical MRTD Data" as follows:

- 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-CAM
- 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

Application note: Due to interoperability reasons the ICAO DOC 9303 [33] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode if it is accessed using BAC.

User Data transferred between the TOE and the Terminal - *(PACE, EAC1, EAC2)*

All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals. *(Confidentiality, Integrity, Authenticity)*.

3.1.1.1 Refinements relevant for configuration “eDigitialIdentity”

Application note: The access to logical eDigitalIdentity document data contains in the DGx (defined in specification [8]) 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 - *(eID)*

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. *(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 [6] are also applied to sensitive identification use data.

3.1.2 Secondary Assets

Secondary Assets are strictly compliant with the Secondary Assets decribed in the PPs claimed in Section 2.2. Some Secondary Assets have been reworded or added according to PP0086 [7] and PP0087 [11] in order to make them more generic ("travel document" replaced by "electronic document") and to include additional mechanisms (EAC2, eID), without altering the compliance to claimed PPs.

Accessibility to the TOE Functions and Data only for Authorized Subjects - *(PACE, EAC1, EAC2)*

Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only. *(Availability)*.

Genuineness of the TOE - *(PACE, EAC1, EAC2)*

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. *(Availability).*

Electronic Document Communication Establishment Authorization Data - *(PACE, EAC1, EAC2)*

Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE, and are not send to it. Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy. *(Confidentiality, Integrity)*

Secret Electronic Document Holder Authentication Data - *(EAC2)*

Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (PACE passwords). *(Confidentiality, Integrity)*.

TOE internal Non-Secret Cryptographic Material - *(PACE, EAC1, EAC2)*

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality. *(Integrity, Authenticity)*

TOE internal Secret Cryptographic Keys - *(PACE, EAC1, EAC2)*

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality. *(Confidentiality, Integrity)*.

3.1.2.1 Refinements relevant for configuration “eDigitialIdentity”

eDigitalIdentity document Communication Establishment Authorization Data - *(eID)*

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. *(Confidentiality, Integrity).*

Secret eDigitalIdentity document Holder Authentication Data - *(eID)*

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).*(Confidentiality, Integrity).*

3.2 Subjects

Attacker - *(PACE, EAC1, EAC2)*

A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess at most high attack potential. Note that the attacker might capture any subject role recognized by the TOE.

Country Signing Certification Authority (CSCA) - *(PACE, EAC1, EAC2)*

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 ICAO Doc 9303 [33].

Country Verifying Certification Authority (CVCA) - *(EAC1, EAC2)*

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC1 terminals, EAC2 terminals respectively, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates.

Document Signer (DS) - *(PACE, EAC1, EAC2)*

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificate , see ICAO Doc 9303 [33]. Note that this role is usually delegated to a Personalization Agent.

Document Verifier (DV) - *(EAC1, EAC2)*

An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see TR03110-3 [30].

Electronic Document Holder - *(PACE, EAC1, EAC2)*

A person the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic electronic document. Note that an electronic document holder can also be an attacker.

Electronic Document Presenter - *(PACE, EAC1, EAC2)*

A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker.

Manufacturer - *(PACE, EAC1, EAC2)*

Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.

PACE Terminal - *(PACE, EAC1, EAC2)*

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.

Personalization Agent - *(PACE, EAC1, EAC2)*

An organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic document (optical personalization) and storing them within the electronic document's chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable ICAO Doc 9303 [33], TR03110-3 [30]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer. This subject is sometimes refered as “Administrator” in the curent docuent.

EAC1 Terminal/EAC2 Terminal - *(EAC1, EAC2)*

A terminal that has successfully passed the Terminal Authentication protocol (TA) version 1 is an EAC1 terminal, while an EAC2 terminal needs to have successfully passed TA version 2. 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.

Terminal - *(PACE, EAC1, EAC2)*

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 as neither being authenticated as a PACE terminal nor an EAC1 terminal nor an EAC2 terminal.

3.2.1 Refinements relevant for configuration “eDigitialIdentity”

PACE Terminal - *(eID)*

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.

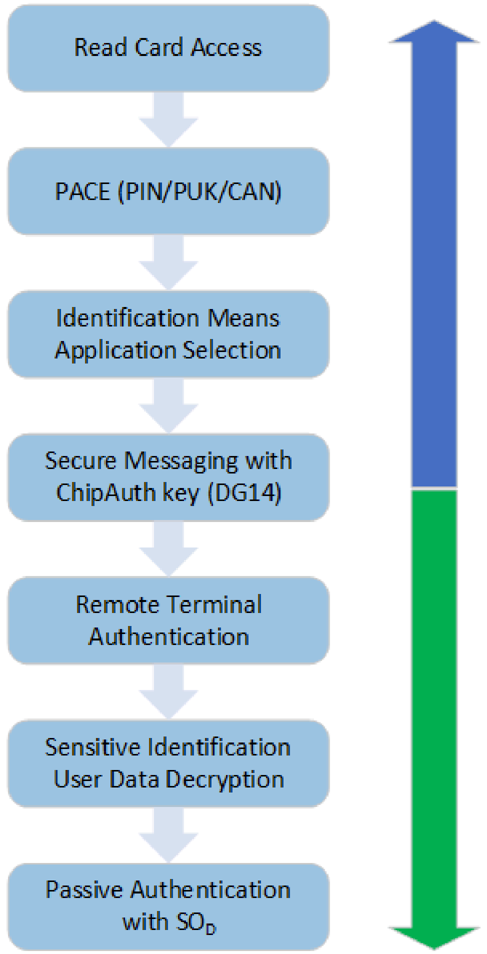
Read Card Access
PACE (PIN/PUK/CAN)
Identification Means Application Selection
Secure Messaging with ChipAuth key (DG14)
Remote Terminal Authentication
Sensitive Identification User Data Decryption
Passive Authentication with SO_D
User side
Remote side

Figure 3. Remote Inspection Procedure

PACE Terminal performs the Remote Inspection Procedure (Figure 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 to ICAO DOC 9303 [33].

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

Administrator - *(GPSCP, CASS)*

A specific kind of user (different from the Electronic Document Holder and Electronic Document Presenter) with TOE administration rights by knowledge of the appropriate Administration authentication keys. The Administrator is the Personalization Agent during the Personalization Phase, and an Administrator ot the TOE during the User Phase.

3.3 Threats

The Threats are strictly compliant with the Threats decribed in the PP(s) claimed in Section 2.2.

Some Threats have been added in order to cover EAC2 additional mechanisms (copied from PP0086 [7]) and the eID configuration (copied from Annexe PP0056v2 eDigitalIdentity [8]), without altering the compliance to claimed PPs.

T.Counterfeit - *Counterfeit of travel document chip data*

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 traveller 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. *(Threat agent: having high attack potential, being in possession of one or more legitimate travel documents. Asset: authenticity of user data stored on the TOE)*

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. [10]) 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. *(Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document. Asset: confidentiality of logical travel document sensitive user data (i.e. biometric reference)*

T.Counterfeit/EAC2 - *Counterfeit of electronic document chip data (EAC2)*

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 a 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.Sensitive_Data - *Unauthorized access to sensitive user data (EAC2)*

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 a legitimate electronic document. Asset: confidentiality of sensitive user data stored on the electronic document)*

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. *(Threat agent: having high attack potential, being in possession of one or more legitimate travel documents. Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document)*

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. *(Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. Asset confidentiality of logical travel document data)*

T.Forgery - *Forgery of Data*

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. *(Threat agent: having high attack potential. Asset: integrity of the travel document)*

T.Information_Leakage -*Information Leakage from travel document*

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.*(Threat agent: having high attack potential. Asset: confidentiality of User Data and TSF-data of the travel document)*

T.Malfunction - *Malfunction due to Environmental Stress*

An attacker may cause a malfunction of the travel document’s hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE’ hardware or to (ii) circumvent, deactivate or modify security functions of the TOE’s Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document’s Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation. *(Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation. Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document)*

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. *(Threat agent: having high attack potential, being in possession of one or more legitimate travel documents. Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document)*

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. *(Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. Asset: confidentiality of logical travel document data)*

T.Tracing - *Tracing travel document*

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. *(Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance. Asset: privacy of the travel document holder)*

T.Sensitive_ID_User_Data - *Unauthorized access to sensitive ID user data (eID)*

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 3.3 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.

3.4 Organisational Security Policies

The OSPs are strictly compliant with the OSPs decribed in the PP(s) claimed in Section 2.2.

Some OSPs have been added in order to cover EAC2 additional mechanisms (copied from PP0086 [7]) and CASS additional mechanism of the eID configuration, without altering the compliance to claimed PPs.

P.Personalisation - *Personalisation of the travel document by issuing State or Organisation only*

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

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.EAC2_Terminal - *Abilities of Terminals executing EAC Version 2 (EAC2)*

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 [29], and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

P.Terminal_PKI - *PKI for Terminal Authentication (EAC2)*

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.Card_PKI - *PKI for Passive Authentication (issuing branch)*

The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}).
2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [33]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [33].
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.Manufact - *Manufacturing of the travel document'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.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 (see Assets).

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, cf. sec. 1.2.3 above.
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.Terminal - *Abilities and trustworthiness of terminals*

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

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [33].
2. They shall implement the terminal parts of the PACE protocol [32], of the Passive Authentication [33] 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 C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [33]).
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.Trustworthy_PKI - *Trustworthiness of PKI*

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

P.CASS_Replacement - *Replacement of Chip Authentication Security Services (CASS)*

The CASS (Chip Authentication keys and related material) can be replaced on request of an authorized user during the Usage phase of the electronic document (phase 7 of the TOE LifeCycle). This can be done in two different ways: i) by activating replacement CASS prepared during the personalization phase of the TOE (prepared replacement CASS) or ii) by uploading new CASS using appropriate commands (uploaded replacement CASS). The replacement of the CASS is considered as a configuration operation of the TOE (no code upload) 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)

3.5 Assumptions

The Assumptions are strictly compliant with the Assumptions decribed in the PPs claimed in Section 2.2.

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.

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 [32] and/or BAC [10]. 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 according to [33].

4 Security Objectives

4.1 Security Objectives for the TOE

The Security Objectives for the TOE are strictly compliant with the Security Objectives for the TOE decribed in the PP(s) claimed in Section 2.2.

Some Security Objectives for the TOE have been extended or added in order to cover EAC2 additional mechanisms (copied from PP0086 [7]), eID configuration (copied from Annexe PP0056v2 eDigitalIdentity [8]), and CASS additional mechanism of the eID configuration, without altering the compliance to claimed PPs.

OT.Chip_Auth_Proof - *Proof of the travel document's chip authenticity*

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in TR03110-1 [28]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

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.Chip_Auth_Proof_PACE_CAM - *Proof of the electronic document's chip authenticity*

The TOE must support the terminals to verify the identity and authenticity of the electronic document's chip as issued by the identified issuing State or Organization by means of the PACE-Chip Authentication Mapping (PACE-CAM) as defined in ICAO Doc 9303 [33]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

OT.AC_Pers_EAC2 - *Personalization of the Electronic Document (EAC2)*

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 the PACE PP [9] as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

OT.CA2 - *Proof of the Electronic Document's Chip Authenticity (EAC2)*

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 [29]). 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.Sens_Data_EAC2 - *Confidentiality of sensitive User Data (EAC2)*

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.AC_Pers - *Access Control for Personalisation 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 (ICAO Doc 9303 [33]) 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.

OT.Data_Authenticity - *Authenticity of Data (extended for EAC2)*

The TOE must ensure authenticity of the User Data and the TSF-data[2] stored on it by enabling verification of their authenticity at the terminal-side[3]. 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)[4].

Application note: This Objective from PACE PP is extended to all kinds of PACE terminals and EAC2 terminals.

OT.Data_Confidentiality - *Confidentiality of Data*

The TOE must ensure confidentiality of the User Data and the TSF-data[5] 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.Data_Integrity - *Integrity of Data (extended for EAC2)*

The TOE must ensure integrity of the User Data and the TSF-data[6] 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.

Application note: This Objective from PACE PP is extended to all kinds of PACE terminals and EAC2 terminals.

OT.Identification - *Identification of the TOE*

[2] where appropriate, see Assets
[3] serification of SO_D
[4] secure messaging after PACE authentication
[5] where appropriate, see Assets
[6] wher appropriate, see Assets

The TOE must provide means to store Initialisation[7] 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).

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 User Data or/and TSF-data stored and/or processed by the travel document

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

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

OT.Prot_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 have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

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.Prot_Phys-Tamper - *Protection against Physical Tampering*

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

- measuring through galvanic contacts representing a direct physical probing on the chip’s surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)

with a prior

[7] among other, IC Identification data

- reverse-engineering to understand the design and its properties and functionality.

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.AA_Proof - *Proof of MRTD's chip authenticity by Active Authentication (AA)*

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 ICAO Doc 9303 [33].

OT.Sens_Ident_User_Data - *Confidentiality of sensitive identification user data (eID)*

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. Note 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 [8] 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 (CASS)*

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 [8]. 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 either during preparation phase (prepared replacement CASS) or during the user phase under restricted acces conditions (uploaded replacement CASS), the objective "O.Security_Service_Provisioning" specified in [8] was not retained (no added value with regard to existing Security Objectives like OT.AC_Pers, OT_AC_PERS_EAC2, or OT.Sens_Data_EAC2).

Nevertheless, the evidence of authenticity and integrity of the commands that triggers the 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 [8] was not retained (no added value with regard to OT.Identification.

4.2 Security Objectives for the operational environment

The Security Objectives for the Operational Environment are strictly compliant with the SOEs decribed in the PPs claimed in Section 2.2.

Some SOEs have been extended or added in order to cover EAC2 additional mechanisms (copied from PP0086 [7]), eID configuration (copied from Annexe PP0056v2 eDigitalIdentity [8]), and CASS additional mechanism of the eID configuration, without altering the compliance to claimed PPs.

OE.Auth_Key_Travel_Document - *Travel document Authentication Key*

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document’s Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or 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.

Justification: This security objective for the operational environment is needed additionally to those from the PACE PP [9] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Protection Profile and not in the PACE PP [9].

OE.Authoriz_Sens_Data - *Authorization for Use of Sensitive Biometric Reference Data*

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

Justification: This security objective for the operational environment is needed additionally to those from PACE PP [9] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in the PACE PP [9].

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 traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [32] and/or the Basic Access Control [33]. 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.

Justification: This security objective for the operational environment is needed additionally to those from PACE PP [9] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in the PACE PP [9] and therefore also counters T.Forgery and A.Passive_Auth from the PACE PP [9]. This is done because a new type of Inspection System is introduced in this PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

OE.Ext_Insp_Systems - *Authorization of Extended Inspection Systems*

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

Justification: This security objective for the operational environment is needed additionally to those from the PACE PP [9] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

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.

Justification: This security objective for the operational environment is needed additionally to those from the PACE PP [9] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Chip_Auth_Key - *Key Pairs needed for Chip Authentication and Restricted Identification (EAC2)*

The electronic document issuer has to ensure that the electronic document’s chip authentication key pair are 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 [29] to check the authenticity of the electronic document's chip.

Justification: The TSF of the PACE PP [9] 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 the PACE PP [9].

OE.Terminal_Authentication - *Key pairs needed for Terminal Authentication (EAC2)*

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.

Justification: The TSF of the PACE PP [9] 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 the PACE PP [9].

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 ICAO Doc 9303 [33]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to ICAO Doc 9303 [33]. 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.Personalisation - *Personalisation of travel document*

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 as defined in ICAO Doc 9303 [33], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in ICAO Doc 9303 [33] (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 ICAO Doc 9303 [33].
2. The related terminals implement the terminal parts of the PACE protocol [32], of the Passive Authentication [32] (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, [33]).
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.

Application note: OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [10].

Application note: Opposite to OE.Terminal from PACE PP [9], a terminal supporting EAC2 according to TR03110-2 [29] needs to store its own credentials for Extended Access Control and (if used) the Restricted Identity.

OE.Electronic_Document_Holder - *Electronic document holder Obligations*

The Electronic 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.Active_Auth_Key_Travel_Document - *Travel document active authentication keys (AA)*

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.CASS_Replacement - *Replacement of Chip Authenticate Security Service (CASS)*

The Personalization agent must follow the ChipDoc v4 ICAO Personalization Guide [14] and ChipDoc v4 User Guidance Manual [12] to prepare the replacement CASS material.

During the user phase, the TOE Administrator must follow the ChipDoc v4 User Guidance Manual [12] to apply the commands for replacement of the CASS (upload of new CASS or subtitution by prepared CASS).

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.

The Security Objectives Rationale is strictly compliant with the Security Objectives Rationales decribed in the PP(s) claimed in Section 2.2.

Some Security Objectives Rationale have been extended or added in order to cover EAC2 additional mechanisms (copied from PP0086 [7]), eID configuration (copied from Annexe PP0056v2 eDigitalIdentity [8]), and CASS additional mechanism of the eID configuration, without altering the compliance to claimed PPs.

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.

Table 6. Mapping of security problem definition to security objectives.

	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE	OT_AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfuntion	OT.Prot_Phys-Tamper	OT.Tracing	OT.CASS_Replacement	OT.AA_Proof	OE.Auth_Key_Travel	OE.Authoriz_Sens_Data	OE_Exam_Travel_Document	OE_Ext_Insp_Systems	OE_Prot_Logical_Travel	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Legislative_Compliance	OE.Passive_Auth_Sign	OE.Personalisation	OE.Terminal	OE.Electronic_Document	OE_Active_Auth_Key_Travel	OE.CASS_Replacement
T.Counterfeit	X		X															X	X		X										X	
T.Read_Sensitive_ Data		X																		X		X										
T.Counterfeit/EAC2					X																			X								
T.Sensitive_Data						X																			X							
T.Abuse-Func												X																				
T.Eavesdropping		X				X			X																							
T.Forgery				X			X	X		X		X			X						X						X	X	X			
T.Information_ Leakage													X																			
T.Malfunction														X																		
T.Phys-Tamper															X																	
T.Skimming		X				X		X	X	X															X					X		
T.Tracing																X														X		
P.Personalisation							X				X																	X				
P.Sensitive_Data		X																		X		X										
P.EAC2_Terminal																								X	X				X			
P.Terminal_PKI																									X							
P.Card_PKI																											X					
P.Manufact											X																					
P.Pre-Operational				X			X				X															X		X				
P.Terminal																					X								X			
P.Trustworthy_PKI																											X					
P.CASS_ Replacement		X					X	X	X	X	X						X															X

Table 6. Mapping of security problem definition to security objectives*....continued*

	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_PACE	OT_AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfuntion	OT.Prot_Phys-Tamper	OT.Tracing	OT.CASS_Replacement	OT.AA_Proof	OE.Auth_Key_Travel	OE.Authoriz_Sens_Data	OE_Exam_Travel_Document	OE_Ext_Insp_Systems	OE_Prot_Logical_Travel	OE.Chip_Auth_Key	OE.Terminal_Authentication	OE.Legislative_Compliance	OE.Passive_Auth_Sign	OE.Personalisation	OE.Terminal	OE.Electronic_Document	OE_Active_Auth_Key_Travel	OE.CASS_Replacement
A.Auth_PKI																				X		X										
A.Insp_Sys																					X		X									
A.Passive_Auth																					X						X					

4.3.2 Security objectives sufficiency

The threat **T.Counterfeit** 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. OT.Chip_Auth_Proof_PACE_CAM ensures that the chip in addition to CA1 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports the same security functionality as CA1 does. PACE-CAM enables much faster authentication of the chip than running PACE with general mapping followed by CA1. The Public Chip Authentication Key has to be written into EF.DG14 (respectively EF.CardSecurity for PACE-CAM) 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 (or PACE-CAM) 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”.

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 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 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 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_Confidentiality through a trusted channel based on PACE Authentication, and by OT.Sens_Data_Conf and OT.Sens_Data_EAC2 demanding a trusted channel that is based on Chip Authentication 1 or 2.

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 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.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_Integrity, OT.Data_Authenticity and OT.Data_Confidentiality through the PACE authentication. the threat is also addressed by OT.Sens_Data_Conf 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.Electronic_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.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.Electronic_Document_Holder (the attacker does not a priori know the correct values of the shared passwords).

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.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 [29], 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.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.Trustworthy_PKI** is enforced by OE.Passive_Auth_Sign (for CSCA, issuing PKI branch).

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 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 assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Passive_Auth_Sign "Authentication of travel document by Signature" from PACE PP [7] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_Travel_Document "Examination of the physical part of the travel document".

4.3.3 Additional Security Objectives Rationale relevant for "eDigitalIdentity" configuration

The following coverage and rationale are only relevant in the context of configuration "eDigitalIdentity"

4.3.3.1 Security Objectives Coverage

Table 7. Mapping of security problem definition to security objectives.

	OT.Sens_Ident_User_ Data_Conf	OT.Sens_Data_Conf	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.CASS_Replacement	OE.CASS_Replacement
T.Skimming	X								
T.Eavesdropping	X								
T.Sensitive_ID_User_Data	X								
P.CASS_Replacement		X	X	X	X	X	X	X	X

4.3.3.2 Security objectives sufficiency

Countering of threats by security objectives:

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 EAC PP [6] and PACE PP [9] 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 EAC PP [6] and PACE PP [9] 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

The following additional families are defined in the PP(s) referenced in Section 2.2

- FAU_SAS Audit data storage
- FCS_RND Generation of random numbers
- FIA_API Authentication Proof of Identity
- FMT_LIM Limited capabilities and availability
- FPT_EMS TOE Emanation

5.1 Definition of the Family FDP_SDC

To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here.

The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

FDP_SDC Stored data confidentiality

Family behaviour:

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component Leveling:

FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1

There are no management activities foressen.

Audit: FDP_SDC.1

There are no actions defined to be auditable.

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*].

6 Security Requirements

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

6.1 Security Functional Requirements

Operations are identified with **Bold** text and a footnote. Operations in braquets "[..]" are provided in a table below the SFR statement. Refinments performed in the Security Target are designated by a **Bold**.

6.1.1 FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer**[8] with the capability to store **the Initialisation and Pre-Personalisation Data**[9] in the audit records.

Application note: Initialisation and Pre-Personalisation Data include the IC Identification Data

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1/[Iter] Cryptographic key generation

FCS_CKM.1.1/ **[Iter]** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Algorithm]**[10] and specified cryptographic key sizes **[Key Size]**[11] that meet the following: **[Standard]**[12].

Table 8. Cryptographic key generation

[Iter]	[Algorithm]	[Key size]	[Standard]
DH	DH PKCS#3 [26]	1024, 1536, 2048, 4096 bits	TR-03110-1 [29] (CA1) TR-03110-2 [29] (PACE, CA2)
	ECDH TR03111 [31]	NIST curves 192, 224, 256, 320, 384 and 521 bits Brainpool curves 192, 224, 256, 320, 384 and 512 bits	
PACE_CAM	PACE-CAM in combination with PACE-GM	See DH	ICOA Doc 9303 [33]

[8] [assignment: *authorised users*]
[9] [assignment: *list of audit information*]
[10] [assignment: *cryptographic key generation algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]

Table 8. Cryptographic key generation *...continued*

[Iter]	[Algorithm]	[Key size]	[Standard]
PUF	AES data protection key generation based on RNG and then protected by PUF	256bits	Platform User Manual [18]
GPSCP	AES key derivation	128, 192, 256 bits	GP_SCP_014 [35]
KP	RSA Key Generation	1024, 1536, 2048, 4096 bits	IEEE 1363 [34]
	ECC Key Generation	192, 224, 256, 320, 384, 521 bits	

6.1.2.2 FCS_CKM.4/ICAO Cryptographic key destruction

FCS_CKM.4.1/ICAO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting old key with new key, zeroization, or flushing of key registers**[13] that meets the following: **none**[14].

Application Note:

- The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC (PACE), after successful run of CA1 (EAC1), after a successful run of CA2 (EAC2).
- The TOE shall destroy the CA2 session keys after detection of an error in a received command by verification of the MAC (EAC2).
- The TOE shall destroy the PACE Session Keys after generation of a CA1 Session Keys and changing the secure messaging to the CA1 Session Keys.
- The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reste-session as required by FDP_RIP.1/ICAO.
- The TOE shall destroy the AES data protection key by flushing the key register.

6.1.2.3 FCS_COP.1/[Iter] Cryptographic Operation

FCS_COP.1.1/**[Iter]** The TSF shall perform **[Cryptographic operation]**[15] in accordance with a specified cryptographic algorithm **[Algorithm]**[16] and cryptographic key sizes **[Key Size]**[17] that meet the following: **[Standard], ICAO-SAC [32] (for PACE),**

[13] [assignment: *cryptographic key destruction method*]
[14] [assignment: *list of standards*]
[15] [assignment: *list of cryptographic operations*]
[16] [assignment: *cryptographic algorithm*]
[17] [assignment: *cryptographic key sizes*]

TR-03110-1 [29] (for EAC1), TR-03110-2 [29]/ TR-03110-3 (for EAC2)[18]

Table 9. Cryptographic operations

[Iteration]	[Cryptographic operation]	[Algorithm]	[Key Size]	[Standard]
SHA	Hashing (All)	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	none	FIPS180-4 [20]
SIG_VER	Digital Signature Verification (TA1, TA2)	RSA PKCS#1v1.5 and RSA-PSS PKCS#1v2.1 with SHA-1, SHA-256, SHA-512	1024, 2048, 3072, 4096 bits	PKCS#1 v1.5 [25] or PKCS#1 PSS [34] and FIPS 180-4 [20]
		ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	up to 521 bits	
SIG_GEN	Digital Signature Generation (AA)	RSA	1024, 2048, 3072, 4096 bits	*ISO/IEC 9796-2 [19]*
		ECDSA	up to 521 bits NIST & BP	*ANSI x9.62 [33]*
SM_ENC	Secure Messaging - encryption and decryption (PACE, CA1, CA2)	TDES in CBC mode AES in CBC mode	112 bits (TDES) 128, 192, 256 bits (AES)	FIPS 46-3 (DES)[22] FIPS 197 (AES)[21]
SM_MAC	Secure Messaging - message authentication code (PACE, CA1, CA2)	Retail-MAC CMAC	112 bits (Retail-MAC) 128, 192, 256 bits (CMAC)	FIPS 46-3 (DES)[22] and ISO 9797-1 (Retail MAC) [27] FIPS 197 (AES) [21], SP800-38B (CMAC) [24]
PACE_CAM	PACE-CAM protocol (PACE)	PACE-CAM	128, 192, 256 bits (AES)	TR03110-2 [29]
PUF_ENC	Encryption/ Decription using PUF protected AES data protection key (All)	EAS-CBC	256 bits (AES data protection key)	FIPS 197 (AES)[21] NIST SP800-38A [23]
SYM_AUTH	Symetric authentication (All)	TDES AES	112 bits (TDES) 128, 192, 256 bits (AES)	FIPS 46-3 (DES)[22] FIPS 197 (AES)[21]
GPSCP_ ENC	Secure Messaging - encryption and decryption (GPSCP/Manage platform secure mode)	AES in CBC mode	128, 192, 256 bits	GPC_SPE_014 [35]

[18] [assignment: *list of standards*]

Table 9. Cryptographic operations *...continued*

[Iteration]	[Cryptographic operation]	[Algorithm]	[Key Size]	[Standard]
GPSCP_ MAC	Secure Messaging - message authentication code (GPSCP/Manage platform secure mode)	CMAC	128, 192, 256 bits	GPC_SPE_014 [35]
GPSCP_ AUTH	Mutual Authentication	AES	128, 192, 256 bits	GPC_SPE_014 [35]

6.1.2.4 FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **AIS31 class DRG.4**[19].

Application note This SFR requires the TOE to generate random numbers used for the authentication protocols PACE and CA2 as required by FIA_UAU.4.

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_ACC.1/TRM Subset access control

FDP_ACC.1.1/TRM The TSF shall enforce the **Access Control SFP**[20] on **terminals gaining access to the User Data and data stored in EF.SOD of the electronic document**[21].

Application note: For eDigitalIdentity configuration, the "electronic document" is to be read as "eDigitalIdentity document".

6.1.3.2 FDP_ACF.1/TRM Security attribute based access control

FDP_ACF.1.1/TRM The TSF shall enforce the **Access Control SFP** [22] to objects based on the following:

1. **Subjects:**
   a. Terminal,
   b. PACE terminal,
   c. EAC1 terminal,
   d. EAC2 terminal.
2. **Objects:**

[19] [assignment: *a defined quality metric*]
[20] [assignment: *access control SFP*]
[21] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[22] [assignment: *access control SFP*]

a. all user data stored in the TOE; including sensitive EAC1-protected user data, and sensitive EAC2-protected user data,
b. all TOE intrinsic secret (cryptographic) data.

3. **Security attributes:**

   a. Terminal Authorization Level (access rights)[23]

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 after successful PACE authentication according to TR03110-2 [29], as required by FIA_UAU.1/ ICAO.** [24]

FDP_ACF.1.3/TRM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**[25].

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

1. **Any terminal not being authenticated as a PACE terminal or an EAC2 terminal or an EAC1 terminal is not allowed to read, to write, to modify, or to use any user data stored on the electronic document.**[26]
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 rules:[assignment: list of rules for PIN management chosen from TR03110-2 [29].**
5. **No subject is allowed to read, write, modify, or use the private Restricted Identification key(s) and Chip Authentication key(s) stored on the electronic document.**
6. **Reading, modifying, writing, or using sensitive user data that are protected only by EAC2, is allowed only to EAC2 terminals using the following mechanism:The TOE applies the EAC2 protocol (cf. FIA_UAU.5/ICAO) to determine access rights of the terminal according to TR03110-2 [29]. To determine the effective authorization**

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

[24] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[25] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[26] note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.

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/TRM.**
8. **No subject is allowed to read sensitive user data that are protected only by EAC1, except an EAC1 terminal (OID inspection system) after EAC1, cf. FIA_UAU.1/ICAO, that has a corresponding relative authorization level. This includes in particular EAC1-protected user data DG3 and DG4 from an ICAO-compliant ePass application, cf. TR03110-1 [28] and ICAO Doc 9303 [33].**
9. **If sensitive user data is protected both by EAC1 and EAC2, no subject is allowed to read those data except EAC1 terminals or EAC2 terminals that access these data according to rule 6 or rule 8 above.**
10. **Nobody is allowed to read the private signature key(s)**[27].

6.1.3.2.1 FDP_ACF.1/TRM_eID refinment relevent for eDigitalIdentity configuration

FDP_ACF.1.1/ TRM_eID

The TSF shall enforce the **Access Control SFP** [28] to objects based on the following:

1. **Subjects:**
   a. Terminal,
   b. PACE terminal,
   c. EAC1 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) data stored in the eDigitalIdentity document.
3. **Security attributes:**
   a. Terminal Authorization Level (access rights),
   b. Authentication status of the electronic document holder as a signatory (if an eSign application is included
   c. Chip Authentication v1,[29].

[27] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[28] [assignment: *access control SFP*]
[29] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2/TRM_eID

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_eID after at least successful PACE authentication according to TR03110-2 [29] and/or ICAO Doc 9303 [33], as required by FIA_UAU.1/ICAO.**
- **A PACE Terminal is allowed to read data objects 2a) of FDP_ACF.1.1/TRM_eID according to [38] only after a successful PACE authentication followed by Chip Authentication v1 as required by FIA_UAU.1/ICAO. 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_eID according to [38] only after a successful PACE authentication followed by Chip Authentication v1 and Terminal Authentication v1 as required by FIA_UAU.1/ICAO.**[30]

FDP_ACF.1.3/TRM_eID

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**[31].

FDP_ACF.1.4/TRM_eID

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

1. **Any terminal not being authenticated at least as PACE terminal is not allowed to read, to write, to modify, or to use any user data stored on the eDigitalIdentity document.**
2. **Terminals not using secure messaging are not allowed to read, write, modify, or 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_eID.**
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_eID.**
5. **Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM_eID,**
6. **Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4**[32].

[30] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[31] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

[32] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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

6.1.3.3 FDP_UCT.1/TRM Basic data exchange confidentiality

FDP_UCT.1.1/TRM The TSF shall enforce the **Access Control SFP**[33] to be able to **transmit and receive** [34]user data in a manner protected from unauthorised disclosure.

6.1.3.4 FDP_UIT.1/TRM Data exchange integrity

FDP_UIT.1.1/TRM The TSF shall enforce the **Access Control SFP**[35] to be able to transmit and receive[36] user data in a protected manner from **modification, deletion, insertion and replay**[37] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay**[38] has occurred.

6.1.3.5 FDP_RIP.1/ICAO Subset residual information protection

FDP_RIP.1.1/ICAO The TSF shall ensure that any previous information content of a resource is made unavailable upon the **de-allocation of the resource from**[39] the following objects:

1. **Session Keys (PACE, CA1, CA2) (immediately after closing related communication session),**
2. **the ephemeral private key ephem-SK$_{PICC}$-PACE (by having generated a DH shared secret K),**
3. **secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more)**[40].

Application note: Item 3. applies for eDigitalIdentity configuration

6.1.3.6 FDP_RIP.1/CASS Subset residual information protection

FDP_RIP.1.1/CASS The TSF shall ensure that any previous information content of a resource is made unavailable upon the **de-allocation of the**

[33] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[34] [selection: *transmit, receive*]
[35] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[36] [selection: *transmit, receive*]
[37] [selection: *modification, deletion, insertion, replay*]
[38] [selection: *modification, deletion, insertion, replay*]
[39] [selection: *allocation of the resource to, deallocation of the resource from*]
[40] [assignment: *list of objects*]

resource from[41] the following objects: **Chip Authentication 1 or 2 Security Service**[42] .

6.1.3.7 FDP_RIP.1/PUF Subset residual information protection

FDP_RIP.1.1/PUF The TSF shall ensure that any previous information content of a resource is made unavailable upon the **de-allocation of the resource from**[43] the following objects: **AES data protection key**[44] .

6.1.3.8 FDP_SDC.1/PUF Stored data confidentiality

FDP_SDC.1.1/PUF The TSF shall ensure the confidentiality of the information of the user data while it is stored in the **Elementary Files (EF) if enabled at EF creation**[45].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1/[Iter] Authentication failure handling

FIA_AFL.1.1/**[Iter]** The TSF shall detect when **[N]**[46] unsuccessful authentication attempts occure related to **[Authentication events]**][47].

FIA_AFL.1.2/**[Iter]** When the defined number of unsuccessful authentication attempts has been **met**[48], the TSF shall **[Perform actions]**[49].

Table 10. Authentication failure handlingn

[Iter]	[N]	[Authentication events]	[Perform actions]
PACE	1	Authentication attempts using the PACE **MRZ or CAN** password as shared password	Exponentially increase the reaction time of the TOE to the next authentication attempt using PACE passwords (MRZ, CAN)

[41] [selection: *allocation of the resource to, deallocation of the resource from*]
[42] [assignment: *list of objects*]
[43] [selection: *allocation of the resource to, deallocation of the resource from*]
[44] [assignment: *list of objects*]
[45] [assignment: *memory area*]
[46] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[47] [assignment: *list of authentication events*]
[48] [selection: *met, surpassed*]
[49] [assignment: *list of actions*]

Table 10. Authentication failure handlingn*...continued*

[Iter]	[N]	[Authentication events]	[Perform actions]
Suspend_PIN	An administrator configurable positive integer within [0-14][1]	Consecutive failed authentication attempts using the **Default PACE** PIN **or PUK** as shared password for PACE	Suspend the reference value of the **Default PACE** PIN **or PUK** according to TR03110-2 [29]
Block_PIN	1	Consecutive failed authentication attempts using the suspended **Default PACE** PIN **or PUK** as a shared password for PACE **after a successfull PACE CAN**	Block the reference value of **Default PACE** PIN **or PUK** according to TR03110-2 [29]
Block_Arbitrary_PIN	an administrator configurable positive integer within [1-15]	Consecutive failed authentication attempts using an Arbitrary PIN or PUK as the shared password for PACE	Block the Arbitrary PIN or PUK
Block_Auth	an administrator configurable positive integer within [1-15]	Consecutive failed VERIFY authentication attempts using an Arbitrary PIN, a global CVM PIM, Biometric Finger 1:1/1:N or Biometric Face Data	Block the PIN or Biometric Object
Block_Sym	an administrator configurable positive integer within [1-15] or Infinite	Consecutive failed EXTERNAL AUTHENTICATION attempts using Symmetric Authentication Key	Block the Symetric Authentication Key
Block_PA	1	Consecutive failed EXTERNAL AUTHENTICATION attempts using Personalization Agent Key	

[1] "0" means that the Default PACE PIN or PUK is Suspended by default and so can only be used through PACE CAN with nested PACE PIN allowing only one try before blocking (see FIA_AFL.1.2/Block_PIN).

6.1.4.2 FIA_API.1/[Iter] Authentication proof of identity

FIA_API.1.1/**[Iter]** The TSF shall provide a **[authentication mechanism]**[50] to prove the identity of the **TOE**[51]

[50] [assignment: *authentication mechanism*]

[51] [assignment: *authorized user or rule*]

Table 11. Authentication Mechnism

[Iter]	[Authentication mechanism]
AAP	Active Authentication Protocol according to ICAO Doc 9303 [33]
CA1	Chip Authentication Protocol Version 1 according to TR03110-1 [28]
CA2	Chip Authentication Protocol Version 2 according to TR03110-2 [29] [30]
PACE_CAM	PACE-CAM protocol according to ICAO Doc 9303 [33]

6.1.4.2.1 FIA_API.1/eID eDigitalIdentity Authentication proof of identity

FIA_API.1.1/eID The TSF shall provide **an authentication mechanism**[52] to prove the identity of **the eDigitalIdentity holder**.[53]

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 eDigitalIdentity Document holder itself by presenting its PIN or Biometric Data to the TOE.

6.1.4.3 FIA_UID.1/ICAO Timing of Identification

FIA_UID.1.1/ICAO The TSF shall allow

1. **to establish a communication channel**
2. **carrying out the PACE protocol according to TR03110-2 [29],**
3. **to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS**
4. **carrying out the Chip Authentication Protocol v.1 according to TR03110-1 [28] or the Chip Authentication Mapping (PACE-CAM) according to ICAO Doc 9303 [33]**
5. **carrying out the Terminal Authentication Protocol v.1 according to TR03110-1 [28] or according to ICAO Doc 9303 [28] if PACE-CAM is used**
6. **carrying out the Terminal Authentication protocol 2 according to TR03110-2 [29]**
7. **to carry out the Active Authentication Mechanism**[54]

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

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

[52] [assignment: *authentication mechanism*]
[53] [assignment: *authorized user or rule*]
[54] [assignment: *list of TSF-mediated actions*]

6.1.4.4 FIA_UID.1/GPSCP Timing of Identification

FIA_UID.1.1/GPSCP The TSF shall allow

1. **to establish a communication channel**
2. **carrying out the Mutual Authentication protocol according to GPC_SPE_014 [35]**[55]

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 TOE Administrator having knowledge of the static SCP03 keys allowing the initiation of the SCP (typically the Manufacturer, Pre-personalizer, Personalizer, Administrator in the field).

6.1.4.5 FIA_UAU.1/ICAO Timing of Authentication

FIA_UAU.1.1/ICAO The TSF shall allow

1. **to establish a communication channel,**
2. **carrying out the PACE protocol according to TR03110-2 [29] ,**
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. **carrying out the Chip Authentication Protocol v1 according to TR03110-1 [28] or the Chip Authentication Mapping (PACE-CAM) according to ICAO Doc 9303 [33]**
6. **carrying out the Terminal Authentication Protocol v1 according to TR03110-1 [28] or according to ICAO Doc 9303 [28] if PACE-CAM is used**
7. **carrying out the Terminal Authentication protocol v2 according to TR03110-2 [29]**[56]

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

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

[55] [assignment: *list of TSF-mediated actions*]

[56] [assignment: *list of TSF-mediated actions*]

6.1.4.6 FIA_UAU.1/GPSCP Timing of Authentication

FIA_UAU.1.1/ GPSCP

The TSF shall allow

1. **to establish a communication channel,**
2. **carrying out the Mutual Authentication protocol according to GPC_SPE_014 [35]**[57]

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 TOE Administrator having knowledge of the static SCP03 keys allowing the initiation of the SCP (typically the Manufacturer, Pre-personalizer, Personalizer, Administrator in the field).

6.1.4.7 FIA_UAU.4/ICAO Single-use authentication of the Terminals by the TOE

FIA_UAU.4.1/ICAO

The TSF shall prevent reuse of authentication data related to

1. **PACE protocol according TR03110-2 [29],**
2. **Authentication Mechanism based on AES and TDES**.
3. **Active Authentication Protocol**.
4. **Terminal Authentication 1 protocol according to TR03110-1 [28]**.
5. **Terminal Authentication 2 protocol according to TR03110-2 [29]**[58].

6.1.4.8 FIA_UAU.5/ICAO Multiple Authentication Mechanisms

FIA_UAU.5.1/ICAO

The TSF shall provide

1. **PACE protocol according to TR03110-2 [29] and PACE-CAM protocol according to ICAO Doc 9303 [33],**
2. **Secure messaging according to TR03110-3 [30],**
3. **Passive authentication,**
4. **Symetric Authentication Mechanism based on AES and TDES,**
5. **Terminal Authentication 1 protocol according to TR03110-1 [28].**
6. **Terminal Authentication 2 protocol according to TR03110-2 [29].**

[57] [assignment: *list of TSF-mediated actions*]

[58] [assignment: *identified authentication mechanism(s)]*

7. **Chip Authentication 2 protocol according to TR03110-2 [29]**[59]

to support user authentication.

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

1. **Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.**
2. **The TOE accepts the authentication attempt as personalization agent by the Authentication Mechanism with Personalization Agent Key(s)**
3. **After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.**
4. **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1, or if the terminal uses the public key presented during PACE-CAM and the secure messaging established during PACE**
5. **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 the 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.**
6. **Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by Chip Authentication 2**[60].

6.1.4.9 FIA_UAU.6/ICAO Re-authentication of the Terminal by the TOE

FIA_UAU.6.1/ICAO The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after a successful run of PACE, Chip Authentication 1, Chip Authentication 2 shall be verified as being sent respectively by the PACE terminal, the Inspection System, or the EAC2 terminal**[61].

[59] [assignment: *identified authentication mechanism(s)]*

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

[61] [assignment: *identified authentication mechanism(s)]*

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1/CASS Management of security functions behaviour

FMT_MOF.1.1/ CASS

The TSF restrict the ability to **modify the behavior of**[62] the functions **Chip Authentication 1 or 2**[63] to **the Administrator** [64]

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)

6.1.5.2 FMT_MTD.1/[Iter] Management of TSF data

FMT_MTD.1.1/**[Iter]**

The TSF shall restrict the ability to **[OP]**[65] the **[TSF Data]**[66] to **[Role]**[67]

Table 12. Management of TSF data

[Iter]	[OP]	[TSF Data]	[Role]
CVCA_INI	write	1. initial CVCA Public Key, 2. meta-data of the initial CVCA Certificate as required in TR03110-2 [29], resp. TR03110-3 [30], 3. initial Current Date	the Personalization Agent
CVCA_UPD	update	1. CVCA Public Key (PK_{CVCA}), 2. meta-data of the initial CVCA Certificate as required in TR03110-2 [29], resp. TR03110-3 [30],	the Country Verifying Certification Authority
DATE	modify	the current date	1. CVCA, 2. Document Verifier, 3. EAC1 terminal and EAC2 terminal possessing an Accurate Terminal Certificate according to TR03110-3 [30].
KEY_WRITE	write	Document Basic Access Keys	the Personalization Agent

[62] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[63] [assignment: *list of functions*]
[64] [assignment: *the authorised identified roles*]
[65] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[66] [assignment: *list of TSF data*]
[67] [assignment: *the authorized identified roles*]

Table 12. Management of TSF data ***...continued***

[Iter]	[OP]	[TSF Data]	[Role]
AAPK	load	Active Authentication Private Key	the Personalization Agent
PA	write	card/chip security object(s) (SO_C) and the document Security Object (SO_D)	the Personalization Agent
SK_PICC (a.k.a. CAPK)	create or load	Chip Authentication 1&2 private key(s) (SK_{PICC})	the Personalization Agent
KEY_READ	read	1. PACE passwords, 2. Personalization Agent Keys, 3. Chip Authentication 1&2 private key(s) (SK_{PICC}), 4. Active Authentication private key(s).	none
Initialize_PINPUK	write	initial PIN, PUK, and Biometric Finger 1:1/1:N or Face Data	the Personalization Agent
Change_PIN	change	blocked PIN, PUK, and Biometric Finger 1:1/1:N or Face Data	Electronic Document Holder
Resume_PINPUK	resume	suspended **Default PACE** PIN or PUK	Electronic Document Holder
Unblock_PIN	unblock	blocked PIN, PUK, and Biometric Finger 1:1/1:N or Face Data	1. Electronic Document Holder (using the PUK for unblocking), 2. EAC2 terminal of a type that has the terminal authorization level for PIN management.
Activate_PIN	activate and deactivate	PIN	EAC2 terminal of a type that has the terminal authorization level for PIN management
INI_ENA	write	Initialisation Data and Pre-personalisation Data	Manufacturer
INI_DIS	read out	Initialisation Data and Pre-personalisation Data	Personalization Agent

6.1.5.3 FMT_MTD.1/CASS Management of TSF data

FMT_MTD.1.1/ CASS

The TSF shall restrict the ability to **replace**[68] the **Chip Authentication 1&2 Security Service**[69] to **the Administrator** [70] .

[68] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[69] [assignment: *list of TSF data*]

[70] [assignment: *the authorized identified roles*]

Application note: By changing 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)

6.1.5.4 FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for **TSF data of the Terminal Authentication Protocol v1, Terminal Authentication Protocol v2, and the Access Control SFP**[71].

Application note: "secure value" refers here to the certificate chain validation according to TR03110-3 [30]

6.1.5.5 FMT_LIM.1 Limited capabilities

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 do not allow

1. **User Data to be manipulated and disclosed,**
2. **TSF data to be manipulated and disclosed,**
3. **Software to be reconstructed,**
4. **Substantial information about construction of TSF to be gathered which may enable other attacks,**
5. **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.**[72].

6.1.5.6 FMT_LIM.2 Limited availability

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 do not allow:

1. **User Data to be manipulated and disclosed,**
2. **TSF data to be manipulated and disclosed,**
3. **Software to be reconstructed,**
4. **Substantial information about construction of TSF to be gathered which may enable other attacks,**
5. **sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.**[73].

[71] [assignment: *list of TSF data*]

[72] [assignment: *Limited capability and availability policy*]

[73] [assignment: *Limited capability and availability policy*]

6.1.5.7 FMT_SMF.1/ICAO Specification of Management Functions

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

1. **Initialization,**
2. **Pre-Personalization,**
3. **Personalization,**
4. **Configuration,**
5. **Initialize, Resume, Unblock, Change the PIN, PUK and Biometric Data (if any), based on defined access rights**
6. **Activate and deactivate the default PACE PIN**
7. [74].

Application note: Items 5. and 6. only apply to eDigitalIdentity application type

6.1.5.8 FMT_SMF.1/CASS Specification of Management Functions

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

1. **Replacement Chip Authentication 1 or 2 Security Service**[75].

6.1.5.9 FMT_SMR.1/ICAO Security roles

FMT_SMR.1.1/ICAO The TSF shall maintain the roles

1. **Manufacturer,**
2. **Personalization Agent,**
3. **Country Verifying Certification Authority,**
4. **Document Verifier,**
5. **Terminal,**
6. **PACE terminal,**
7. **EAC2 terminal,**
8. **EAC1 terminal,**
9. **Administrator,**
10. **Electronic Document Holder.**[76].

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

6.1.6 Protection of the TSF (FPT)

[74] [assignment: *list of management functions to be provided by the TSF*]

[75] [assignment: *list of management functions to be provided by the TSF*]

[76] [assignment: the authorised identified roles]

6.1.6.1 FPT_EMS.1/ICAO TOE Emanation

FPT_EMS.1.1/ICAO The TOE shall not emit **information of IC Power consumption**[77] in excess of **State of the Art values**[78] enabling access to

1. **the session keys for PACE, Chip Authentication 1&2**
2. **the ephemeral private keys for PACE (incl. PACE-CAM)**
3. **the Chip Authentication 1&2 private keys**
4. **the PIN, PUK, Biometric Data**
5. **the Active Authentication Private Key**
6. **the Personalisation Agent Key(s),**[79]

FPT_EMS.1.2/ICAO The TSF shall ensure **any users** are unable to use the following interface **electronic document 's contactless /contact-based interface and circuit contacts** to gain access to

1. **the session keys for PACE, Chip Authentication 1&2**
2. **the ephemeral private keys for PACE (incl. PACE-CAM)**
3. **the Chip Authentication 1&2 private keys**
4. **the PIN, PUK, Biometric Data**
5. **the Active Authentication Private Key**
6. **the Personalisation Agent Key(s),**[80]

6.1.6.2 FPT_FLS.1/ICAO Failure with preservation of secure state

FPT_FLS.1.1/ICAO 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/ICAO,** [81]

6.1.6.3 FPT_FLS.1/CASS Failure with preservation of secure state

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

1. **Failure of the Chip Authentication 1 or 2 Security Service replacement** [82]

[77] [assignment: *types of emissions*

[78] [assignment: *specified limits*]

[79] [assignment: *list of types of TSF data*]

[80] [assignment: *list of types of TSF data*]

[81] [assignment: *list of types of failures in the TSF*]

[82] [assignment: *list of types of failures in the TSF*]

6.1.6.4 FPT_PHP.3/ICAO Resistance to physical attack

FPT_PHP.3.1/ICAO The TSF shall resist **physical manipulation and physical probing**[83]to the **TSF**[84] by responding automatically such that the SFRs are always enforced.

6.1.6.5 FPT_TST.1/ICAO TSF testing

FPT_TST.1.1/ICAO The TSF shall run a suit of self-tests **during initial start-up or before running a secure operation**[85] to demonstrate the correct operation of **the TSF**[86]

FPT_TST.1.2/ICAO The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**[87]

FPT_TST.1.3/ICAO The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**[88]

Application note: Crypto Self-tests are performed by the Operating System during start-up.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_ITC.1/[Iter] Inter-TSF trusted channel

FTP_ITC.1.1/**[Iter]** The TSF shall provide a communication channel between itself and **[Refinment]** 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 shall be established by performing the [Iteration] protocol according to [TR03110-2].**

FTP_ITC.1.2/**[Iter]** The TSF shall permit **[Refinment]** to initiate communication via the trusted channel.

FTP_ITC.1.3/**[Iter]** The TSF shall **enforce** communication via the trusted channel for **[Function]**[89].

[83] [assignment: *physical tampering scenarios*]

[84] [assignment: *list of TSF devices/elements*]

[85] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: condictions under which self test should occur]*]

[86] [selection: *[assignment: parts of the TSF], the TSF*]

[87] [selection: *[assignment: parts of TSF data], TSF data*]

[88] [selection: *[assignment: parts of TSF], TSF*]

[89] [assignment: *list of other functions for which a trusted channel is required*]

Table 13. Inter-TSF trusted channels

[Iter]	[Refinment]	[Function]	[Standard]
PACE	a PACE terminal	any data exchange between the TOE and a PACE terminal after PACE	ICAO Doc 9303 [33] or TR03110-2 [29]
CA1	an EAC1 terminal	any data exchange between the TOE and an EAC1 terminal after Chip Authentication 1	TR03110-1 [28]
CA2	an EAC2 terminal	any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2	TR03110-2 [29]

6.2 Security Functional Requirements Rationale

6.2.1 Security Requirement Coverage

The following table indicates the association of the security requirements and the security objectives of the TOE. Some requirements correspond to the security objectives of the TOE in combination with other objectives.

Table 14. Mapping of security problem definition to security objectives

TOE SFRs / TOE Security Objectives	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.AA_Proof	OT.Sens_Ident_User_	OT.CASS_Replacement	Intentionally left blanc	Intentionally left blanc
FAU_SAS.1				x			x				x										
FCS_CKM.1/DH	x	x			x	x	x	x	x	x											
FCS_CKM.1/PACE_CAM			x					x	x	x											
FCS_CKM.1/KP																	x				
FCS_CKM.1/PUF													x		x						
FCS_CKM.1/GPSCP		x		x				x	x	x									x		
FCS_CKM.4/ICAO		x				x	x	x	x	x											
FCS_COP.1/SHA					x	x		x	x	x							x				
FCS_COP.1/SIG_GEN																	x				
FCS_COP.1/SIG_VER		x				x	x														
FCS_COP.1/SM_ENC	x	x				x	x		x										x		
FCS_COP.1/SM_MAC	x	x			x		x	x		x									x		
FCS_COP.1/PACE_CAM			x					x	x	x											

Table 14. Mapping of security problem definition to security objectives*...continued*

TOE SFRs / TOE Security Objectives	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.AA_Proof	OT.Sens_Ident_User_	OT.CASS_Replacement	Intentionally left blanc	Intentionally left blanc
FCS_COP.1/PUF_ENC													x		x						
FCS_COP.1/SYM_AUTH							x														
FCS_COP.1/GPSCP_AUTH		x		x				x	x	x									x		
FCS_COP.1/GPSCP_ENC		x							x										x		
FCS_COP.1/GPSCP_MAC								x		x									x		
FCS_RND.1		x			x	x	x	x	x	x							x				
FDP_ACC.1/TRM		x		x		x	x		x	x											
FDP_ACF.1/TRM		x		x		x	x		x	x											
FDP_ACF.1/TRM_eID		x					x		x	x											
FDP_RIP.1/ICAO				x	x	x		x	x	x											
FDP_RIP.1/CASS																			x		
FDP_RIP.1/PUF													x								
FDP_SDC.1/PUF													x		x						
FDP_UCT.1/TRM		x				x			x	x											
FDP_UIT.1/TRM						x			x	x											
FIA_AFL.1/PACE																x					
FIA_AFL.1/Suspend_PIN				x		x		x	x	x											
FIA_AFL.1/Block_PIN				x		x		x	x	x						x					
FIA_AFL.1/Block_Arbitrary_ PIN				x		x		x	x	x											
FIA_AFL.1/Block_Auth																		x			
FIA_AFL.1/Block_Sym						x															
FIA_AFL.1/Block_PA							x														
FIA_API.1/AAP																			x		
FIA_API.1/CA1	x	x						x	x	x											
FIA_API.1/CA2					x	x		x	x	x											
FIA_API.1/PACE_CAM			x					x	x	x											
FIA_API.1/eID																		x			
FIA_UID.1/ICAO		x	x	x		x	x	x	x	x									x		
FIA_UID.1/GPSCP		x		x				x	x	x									x		
FIA_UAU.1/ICAO		x		x		x	x	x	x	x									x		

Table 14. Mapping of security problem definition to security objectives*...continued*

TOE SFRs / TOE Security Objectives	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.AA_Proof	OT.Sens_Ident_User_	OT.CASS_Replacement	Intentionally left blanc	Intentionally left blanc
FIA_UAU.1/GPSCP		x		x				x	x	x									x		
FIA_UAU.4/ICAO		x				x	x	x	x	x											
FIA_UAU.5/ICAO		x	x			x	x	x	x	x											
FIA_UAU.6/ICAO		x				x	x	x	x	x											
FMT_LIM.1												x									
FMT_LIM.2												x									
FMT_MOF.1/CASS																			x		
FMT_MTD.1/AAPK																	x				
FMT_MTD.1/CVCA_INI		x				x		x	x	x											
FMT_MTD.1/CVCA_UPD		x				x		x	x	x											
FMT_MTD.1/DATE		x				x		x	x	x											
FMT_MTD.1/KEY_WRITE		x					x														
FMT_MTD.1/PA				x	x	x	x	x	x	x											
FMT_MTD.1/SK_PICC	x	x			x	x		x	x	x											
FMT_MTD.1/KEY_READ	x	x		x	x	x	x	x	x	x											
FMT_MTD.1/Initialize_ PINPUK				x		x		x	x	x											
FMT_MTD.1/Change_PIN				x		x		x	x	x											
FMT_MTD.1/Resume_ PINPUK				x		x		x	x	x											
FMT_MTD.1/Unblock_PIN				x		x		x	x	x											
FMT_MTD.1/Activate_PIN				x		x		x	x	x											
FMT_MTD.1/INI_ENA				x			x				x										
FMT_MTD.1/INI_DIS				x			x				x										
FMT_MTD.1/CASS																			x		
FMT_MTD.3		x				x		x	x	x											
FMT_SMF.1/ICAO	x			x		x	x	x	x	x	x										
FMT_SMF.1/CASS																			x		
FMT_SMR.1/ICAO	x			x		x	x	x	x	x	x								x		
FPT_EMS.1/ICAO							x						x								
FPT_FLS.1/ICAO													x	x							

Table 14. Mapping of security problem definition to security objectives...*continued*

TOE SFRs / TOE Security Objectives	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.Chip_Auth_Proof_	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.AA_Proof	OT.Sens_Ident_User_	OT.CASS_Replacement	Intentionally left blanc	Intentionally left blanc
FPT_FLS.1/CASS																			x		
FPT_PHP.3/ICAO										x			x		x						
FPT_TST.1/ICAO													x	x							
FTP_ITC.1/PACE						x		x	x	x						x					
FTP_ITC.1/CA1								x	x	x						x					
FTP_ITC.1/CA2						x		x	x	x						x					

6.2.2 Security Requirements Sufficiency

OT.Chip_Auth_Proof

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/CA1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/DH is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/SK_PICC and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [28] requires additional TSF according to FCS_CKM.1/DH (for the derivation of the session keys), FCS_COP.1/SM_ENC and FCS_COP.1/SM_MAC (for the ENC_MAC_Mode secure messaging). The SFRs FMT_SMF.1/ICAO and FMT_SMR.1/ICAO support the functions and roles related.

OT.Sense_Data_Conf

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM, FDP_ACF.1/TRM_eID 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/ICAO and FIA_UAU.1/ICAO require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/ICAO requires the successful Chip Authentication v.1 (FIA_API.1/CA1) 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/ICAO. The SFR FIA_UAU.6/ICAO 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/DH (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/SM_ENC and FCS_COP.1/SM_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4/ICAO after use. The SFR FMT_MTD.1/SK_PICC and

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

The Personalization Agent and Administrator 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 ensures 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.

OT.Chip_Auth_Proof_PACE_CAM

The security objective **OT.Chip_Auth_Proof_PACE_CAM** aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol. This is supported by FCS_CKM.1/PACE_CAM for cryptographic key-generation, and FIA_API.1/PACE_CAM and FCS_COP.1/PACE_CAM for the implementation itself, as well as FIA_UID.1/ICAO and FIA_UAU.5/ICAO, the latter supporting the PACE protocol.

OT.AC_Pers_EAC2

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/ICAO and FIA_UAU.1/ICAO. The SFRs FMT_SMF.1/ICAO and FMT_SMR.1/ICAO 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/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN, FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, and FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PINPUK) also support the achievement of this objective. FDP_RIP.1/ICAO 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 with respect to the pre-personalization data. FMT_MTD.1/PA covers the related property of OT.AC_Pers_EAC2 (writing/updating SO_C and SO_D 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 can not be read by users.

The SCP03 allows administration of the TOE during the user phase 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, FCS_COP.1/GPSCP_AUTH, FIA_AFL.1/Block_Sym.

OT.CA2

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/CA2 using FCS_CKM.1/DH. CA2 provides an evidence of possessing the Chip Authentication

Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, whereas FMT_MTD.1/KEY_READ requires making this key unreadable by users. Hence, its value remains confidential. FDP_RIP.1/ICAO requires erasing the values of SK_{PICC} and the session keys, here for CMAC.The authentication token T_{PICC} is calculated using FCS_COP.1/SM_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 SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified by the personalization agent. Hence is to consider as trustworthy.

OT.Sens_Data_EAC2

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/TRM. A specific authorization level is achieved by terminal identification/ authentication as required by the SFRs FIA_UID.1/ICAO, FIA_UAU.1/ICAO, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/ICAO, FIA_UAU.1/ICAO, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/ Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN,FMT_MTD.1/ Resume_PINPUK, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Activate_PIN) also support to achieve this objective. FDP_RIP.1/ICAO requires erasing the temporal values of the PIN and PUK. FIA_UAU.4/ICAO, FIA_UAU.5/ICAO, FIA_UAU.6/ICAO and FCS_CKM.4/ICAO 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/PACE and FTP_ITC.1/CA2 using FCS_COP.1/SM_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 2, cf. FIA_API.1/CA2 using FCS_CKM.1/ DH and possessing the special properties FIA_UAU.5/ICAO, and FIA_UAU.6/ICAO. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/ICAO, FIA_UAU.1/ICAO and FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, FIA_UAU.6/ICAO.

CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value remains confidential. FDP_RIP.1/ICAO requires erasing the values of SK_{PICC} and session keys, here for K_{ENC}. FMT_MTD.1/PA requires that only the the personalization agent is allowed to modify the SO_C (containing amongst other, the signature of PK_{PICC}) 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/ICAO and FMT_SMR.1/ICAO support the related functions and roles.

OT.AC_Pers

The security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document” addresses the access control of the writing the logical travel document. During the personalization phase the personalization agent authenticates as per FIA_UAU.5/ICAO (symetric auth.) supported by FCS_COP.1/SYM_AUTH. 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 with respect to the Pre-personalisation Data. During the personalization phase, The write access to the logical travel document data are defined by the SFR FIA_UID.1/ICAO, FIA_UAU.1/ICAO, FDP_ACC.1/TRM, FDP_ACF.1/TRM_eID 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 SO_D and, in generally, personalisation data). The SFR FMT_SMR.1/ICAO lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1/ICAO lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1/ICAO 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/ICAO and FIA_UAU.5/ICAO. If the Personalisation Terminal want 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/DH (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/SM_ENC and FCS_COP.1/PSM_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/ICAO (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), FCS_COP.1/SM_ENC (to verify the authentication attempt), and FIA_AFL.1/Block_PA (to block the Personalization Agent key in case of failed authentication). The session keys are destroyed according to FCS_CKM.4/ICAO 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/ICAO support the related functions. The SFR FDP_RIP.1/ICAO requires erasing the temporal values PIN and PUK.

OT.Data_Authenticity

The security objective **OT.Data_Authenticity** ensures the authenticity of user- and TSF-Data (after PACE, Chip-Terminal Authentication 1, or Terminal-Chip Authentication 2) by enabling its verification on both the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE, FTP_ITC.1/CA1 and FTP_ITC.1/CA2 using FCS_COP.1/SM_MAC. A prerequisite for establishing this trusted channel is a successful PACE, Chip-Terminal Authentication 1, or Terminal-Chip Authentication 2 (cf. FIA_UID.1/ICAO, FIA_UAU.1/ICAO, FIA_API.1/CA1, FIA_API.1/PACE_CAM and FIA_API.1/CA2) using FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, and FIA_UAU.6/ICAO. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/ICAO, FIA_UAU.1/ICAO and FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, FIA_UAU.6/ICAO.

CA1 and CA2 provides an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires to make this key unreadable by users. Hence its value remains confidential. FDP_RIP.1/ICAO requires to erase the values of SK_{PICC} and session keys, here for K_{MAC}.

FMT_MTD.1/PA requires that the SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified only by the personalization agent. Hence is to consider as trustworthy. A prerequisite for successful CA2 is an accomplished TA2 as required by FIA_UID.1/ICAO, FIA_UAU.1/ICAO, supported by FCS_COP.1/SIG_VER. The TA2 protocol uses the result of the PACE authentication (FIA_UID.1/ICAO, FIA_UAU.1/ICAO) being, in turn, supported by FCS_CKM.1/DH. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN,FMT_MTD.1/Resume_PINPUK, MT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Activate_PIN) also support achieving this objective. FDP_RIP.1/ICAO requires to erase the temporal values of the PIN and PUK. FIA_UAU.4/ICAO, FIA_UAU.5/ICAO, FIA_UAU.6/ICAO and FCS_CKM.4/ICAO represent some specific required 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 roles as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent the general required support for cryptographic operations.The SFRs FMT_SMF.1/ICAO and FMT_SMR.1/ICAO support the related functions and roles.

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.

OT.Data_Confidentiality

The security objective **OT.Data_Confidentiality** ensures that the TOE always ensures confidentiality of the user- and TSF-Data stored and, after PACE, Chip-Terminal Authentication 1, or Terminal-Chip Authentication 2, of their exchange.This objective for the data stored is mainly achieved by FDP_ACC.1/TRM, FDP_ACF.1/TRM_eID and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/ICAO, FIA_UAU.1/ICAO, supported by FCS_COP.1/SIG_VER. The EAC1 and EAC2 protocols use the result of the PACE authentication (FIA_UID.1/ICAO, FIA_UAU.1/ICAO, confidentiality of the PACE passwords is ensured by FMT_MTD.1/KEY_READ) being, in turn, supported by FCS_CKM.1/DH. Since PACE can use the PIN as the shared secret, the use and management of the PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN,FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Change_PIN, MT_MTD.1/Initialize_PINPUK, FMT_MTD.1/Activate_PIN) also support to achieve this objective. FDP_RIP.1/ICAO requires erasing the temporal values of the PIN and PUK. FIA_UAU.4/ICAO, FIA_UAU.5/ICAO, FIA_UAU.6/ICAO and FCS_CKM.4/ICAO 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/PACE, FTP_ITC.1/CA1, FIA_API.1/PACE_CAM, FTP_ITC.1/CA2 and using FCS_COP.1/SM_ENC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 1 or Chip Authentication 2, cf. FIA_API.1/CA1 and FIA_API.1/CA2 using FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, and FIA_UAU.6/ICAO. As a prerequisite of this trusted channel, a trusted channel is established with the PACE protocol using FIA_UID.1/

ICAO, FIA_UAU.1/ICAO and FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, FIA_UAU.6/ICAO.

CA1 and CA2 provide an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, FMT_MTD.1/KEY_READ requires making this key unreadable by users. Thus its value remains confidential. FDP_RIP.1/ICAO requires erasing the values of SK_{PICC} and session keys, here for K_{ENC}. FMT_MTD.1/PA requires that only the personalization agent is allowed to modify the SO_C (containing amongst other, the signature of PK_{PICC}) 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/ICAO and FMT_SMR.1/ICAO support the related functions and roles.

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.

OT.Data_Integrity

The security objective **OT.Data_Integrity** ensures that the TOE always ensures integrity of stored user- and TSF-Data and, after PACE, Chip-Terminal Authentication 1, or Terminal-Chip Authentication 2, of these data exchanged (physical manipulation and unauthorized modifying). Physical manipulation is addressed by FPT_PHP.3/ICAO. Unauthorized modifying of the stored data is addressed by FDP_ACC.1/TRM, FDP_ACF.1/TRM_eID and FDP_ACF.1/TRM. Enforcement of the two previous in a protected manner is ensured by FDP_UCT.1/TRM and FDP_UIT.1/TRM. A specific authorization level is achieved by terminal identification/authentication as required by the SFRs FIA_UID.1/ICAO, FIA_UAU.1/ICAO, supported by FCS_COP.1/SIG_VER. The EAC1 and EAC2 protocols use the result of PACE authentication (FIA_UID.1/ICAO, FIA_UAU.1/ICAO) being, in turn, supported by FCS_CKM.1/DH. Since PACE can use the PIN as the shared secret, using and management of PIN (FIA_AFL.1/Suspend_PIN, FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN,FMT_MTD.1/Resume_PINPUK, FMT_MTD.1/Change_PIN, FMT_MTD.1/Unblock_PIN, FMT_MTD.1/Activate_PIN, FMT_MTD.1/Initialize_PINPUK) also support achievement of this objective. FDP_RIP.1/ICAO requires erasing the temporal values of PIN, PUK. FIA_UAU.4/ICAO, FIA_UAU.5/ICAO and FCS_CKM.4/ICAO represent some required 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 update by authorized identified role as required by FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE. Unauthorized modifying of the exchanged data is addressed by FTP_ITC.1/PACE, FTP_ITC.1/CA1, FTP_ITC.1/CA2 and using FCS_COP.1/SM_MAC. A prerequisite for establishing this trusted channel is a successful Chip Authentication 1 or Chip Authentication 2, cf. FIA_API.1/CA1, FIA_API.1/PACE_CAM, FIA_API.1/CA2 using FCS_CKM.1/DH possessing the special properties FIA_UAU.5/ICAO and FIA_UAU.6/ICAO. As a prerequisite of this trusted channel a trusted channel established with the PACE protocol using FIA_UID.1/ICAO, FIA_UAU.1/ICAO and FCS_CKM.1/DH and possessing the special properties FIA_UAU.5/ICAO, FIA_UAU.6/ICAO.

CA1 and CA2 provide an evidence of possessing the Chip Authentication Private Key (SK_{PICC}). FMT_MTD.1/SK_PICC governs creating/loading SK_{PICC}, and FMT_MTD.1/KEY_READ requires SK_{PICC} to be unreadable by users; thus its value remains confidential. FDP_RIP.1/ICAO requires erasing the values of SK_{PICC} and session keys (here: for K_{MAC}). FMT_MTD.1/PA requires that the SO_C (containing amongst other, the signature of PK_{PICC}) used for Passive Authentication is allowed to be modified only by the personalization agent. Hence, is to considered as trustworthy. The SFRs FCS_COP.1/SHA and FCS_RND.1 represent general support required for cryptographic operations. The SFRs FMT_SMF.1/ICAO and FMT_SMR.1/ICAO support related functions and roles.

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.

OT.Identification

The security objective **OT.Identification** addresses the storage of initialization and pre-personalization data in its non-volatile memory. This data includes the IC identification data that uniquely identify the TOE's chip. This is ensured by FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the manufacturer to write initialization and pre-personalization data (including the personalization agent key). The SFR FMT_MTD.1/INI_DIS requires the personalization agent to disable access to initialization and pre-personalization data in the life cycle phase operational use. The SFRs FMT_SMF.1/ICAO and FMT_SMR.1/ICAO support the related functions and roles.

OT.Prot_Abuse-Func

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

OT.Prot_Inf_Leak

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

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

OT.Prot_Malfunction

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by (i) the SFR FPT_TST.1/ICAO 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/ICAO which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

OT.Prot_Phys-Tamper

The security objective **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” is covered by the SFR FPT_PHP.3/ICAO and FDP_SDC.1/PUF, FCS_CKM.1/PUF, FCS_COP.1/PUF_ENC, FDP_RIP.1/PUF.

OT.Tracing

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

1. While establishing PACE communication with CAN, MRZ or PUK (non-blocking authentication / authorization data) by FIA_AFL.1/PACE,
2. while establishing PACE communication using the PIN (blocking authentication data) by FIA_AFL.1/Block_PIN, FIA_AFL.1/Block_Arbitrary_PIN,
3. for listening to PACE communication and for establishing CA1 or CA2 communication (which is of importance if Chip Security Object and PK_{PICC} are card-individual) by FTP_ITC.1/PACE,
4. and for listening to CA1 or CA2 communication (readable and writable user data: document details data, biographic data, biometric reference data) by FTP_ITC.1/CA1 and FTP_ITC.1/CA2.

OT.AA_Proof

The security objective **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.Sens_Ident_User_Data

The security objective **OT.Sens_Ident_User_Data** is covered by FIA_API.1/eID and FIA_AFL.1/Block_Auth that ensures authentication of the eID holder and access grand to the inspection system.

OT.CASS_Replacement

The security objective **OT.CASS_Replacement (Replacement of Chip Authentication Security Service)** is covered by FMT_SMF.1/CASS, FMT_MOF.1/CASS, FMT_MTD.1/CASS, FMT_SMR.1/ICAO ensuring that the TOE supports replacement of Chip Authentication 1&2 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.

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/ICAO, FIA_UID.1/ICAO, FIA_UAU.1/ICAO, FCS_CKM.1/DH, FCS_COP.1/SM_ENC, FCS_COP.1/SM_MAC.

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

6.3 Security Assurance Requirements

The following table lists all security assurance components that are valid for this Security Target.

Table 15. Security Assurance Requirements according to EAL5 augmented

Name		Title
ADV: Devlopment	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	Semiformal 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 life-cycle model
	ALC_TAT.2	Compliance with implementation standards
ASE: Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extendend components definition
	ASE_REQ.2	Derived security requirements
	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

6.4 Security Assurance Requirements Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. 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 with regards to the security measures providing the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The component ALC_DVS.2 has no dependencies.

AVA_VAN.5 *Vulnerability Assessment - Advanced methodical vulnerability analysis*

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

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

7 TOE Summary Specification

7.1 SF.Access Control

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

7.2 SF.Administration

In Initialization Phase, this TSF provides Card initialization and pre-personalization services as per GlobalPlatform. This includes but is not restricted to card initialization, patch loading, applet installation and instantiation.

In Personalization Phase, the Administrator is identified through the relevant access rights and performs administrative activities like initialization of the file system, configuration/personalization of the TOE, activation of PINs. The key used for data protection is generated during the initialization of the file system.

In Usage phase, the Administrator is identified through the relevant access rights and performs administrative activities like Resuming, Unblocking or Deactivating PINs, or like replacing the Chip Authentication keys.

7.3 SF.Active Authentication

Active Authentication is provided by this TSF based on the availability of DG15 in the MRTD's chip information data. This is decided by the Personalization Agent during phase 3 when the LDS is personalized.

7.4 SF.PACE

The PACE-enabled Basic Access System and the MRTD document mutually authenticate by means of a PACE V2 protocol.

7.5 SF.Chip Authentication

This TSF provides the Chip Authentication 1 (alone or mapped within PACE-CAM) and Chip Authentication 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.

7.7 SF.Personalizer Authentication

The Personalization Agent is authenticated by the TOE using its symmetric key.

7.8 SF.Secure Messaging

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

The SF.Secure_Messaging function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device.

7.9 SF.Crypto

This Security Function is responsible for providing cryptographic support to all the other Security Functions including secure key generation and operations on data such as encrypt and sign.

7.10 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 on request of the authorized user having knowledge of the static SCP03 keys (typically the Manufacturer, the Pre-personalizer, the Personalizer, the Issuer…).

NB : contrary to SF.Secure Messaging, the current security function mostly relies on the platform security functionalities as the application just transfers the command to the platform GP framework.

7.11 SF.Protection

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

7.12 SF.Chip Authentication Security Service Replacement

This TSF provides the capability to replace the Chip Authentication 1 and 2 Private Key (and associated material) in the field. This can be done in two ways: i) by uploading new keys and associated material using dedicated key management commands or ii) by replacing the current ADF with a pre-created ADF containing all the keys and DGs pre-configured.

8 Additional Rationale

8.1 Dependencies Rationale

8.1.1 SFR Dependencies

8.1.1.1 SFR Dependencies

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

Table 16. Dependencies of Security Functional Requirements

SFR	Dependencies
FAU_SAS.1	No dependencies
FCS_CKM.1/*	FCS_COP.1/*, FCS_CKM.4/ICAO
FCS_CKM.4/ICAO	FCS_CKM.1/*
FCS_COP.1/*	FCS_CKM.1/*, FCS_CKM.4/ICAO
FCS_RND.1	No dependencies
FDP_ACC.1/TRM	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1/TRM (FMT_MSA.3 not fulfilled but justified)
FDP_UCT.1/TRM	FTP_ITC.1/*, FDP_ACC.1/TRM
FDP_UIT.1/TRM	FTP_ITC.1/*, FDP_ACC.1/TRM
FDP_RIP.1/CASS	No dependencies
FDP_RIP.1/ICAO	No dependencies
FDP_RIP.1/PUF	No dependencies
FDP_SDC.1/PUF	No dependencies
FIA_AFL.1/*	FIA_UAU.1/ICAO
FIA_API.1/*	No dependencies
FIA_UID.1/ICAO	No dependencies
FIA_UID.1/GPSCP	No dependencies
FIA_UAU.1/ICAO	FIA_UID.1/ICAO
FIA_UAU.1/GPSCP	FIA_UID.1/GPSCP
FIA_UAU.4/ICAO	No dependencies
FIA_UAU.5/ICAO	No dependencies
FIA_UAU.6/ICAO	No dependencies
FMT_MOF.1/CASS	FMT_SMF.1/CASS, FMT_SMR.1/ICAO
FMT_MTD.1/CASS	FMT_SMF.1/CASS, FMT_SMR.1/ICAO
FMT_MTD.1/*	FMT_SMF.1/ICAO, FMT_SMR.1/ICAO
FMT_MTD.3	FMT_MTD.1/*

Table 16. Dependencies of Security Functional Requirements*...continued*

SFR	Dependencies
FMT_LIM.1	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1
FMT_SMF.1/ICAO	No dependencies
FMT_SMF.1/CASS	No dependencies
FMT_SMR.1/ICAO	FIA_UID.1/ICAO
FPT_EMS.1/ICAO	No dependencies
FPT_FLS.1/ICAO	No dependencies
FPT_FLS.1/CASS	No dependencies
FPT_PHP.3/ICAO	No dependencies
FPT_TST.1/ICAO	No dependencies
FTP_ITC.1/*	No dependencies

8.1.1.2 Justification of Unsupported Dependencies for Additional Functionalities

The dependency of FDP_ACF.1/TRM to FMT_MSA.3 is not fulfilled but justified: The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

8.1.2 SAR Dependencies

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

Table 17. Dependencies of Security Assurance Requirements (Security Target)

Assurance 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.1, 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.1	ADV_IMP.1
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.2

Table 17. Dependencies of Security Assurance Requirements (Security Target)*...continued*

Assurance Requirement	Dependencies
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
ATA_VAN.5	ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

8.2 Rationale for Extensions

The following extensions are based on the Protection Profile and have all been adopted by the developer of the TOE:

- FAU_SAS.1 'Audit data storage'
- FCS_RND.1 'Generation of random numbers'
- FMT_LIM.1 'Limited capability' and FMT_LIM.2 'Limited availability'
- FPT_EMS.1 'TOE emanation'
- FIA_API.1 'Authentication Proof of Identity'

8.3 PP Claim Rationale

This ST includes all the security objectives and requirements claimed by the claimed Protection Profiles and, all of the operations applied to the SFRs are in accordance with the requirements of these PPs. The security requirements in the ST is a super-set of the requirements from the claimed PPs.

8.3.1 PP compliancy

The TOE is compliant with the representation provided in the ICAO Machine Readable Travel Document Chip with Extended Access Control PP [6] and PACE PP [9].

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 claimed PPs and this ST is a suitable solution to the generic security problem described in the PP.

9 Bibliography

9 . 1 Evaluation documents

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

[5] Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices, version 1.5.1.

[6] Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC V2 PP), certified under the reference BSI-CC-PP-0056-V2-2012-MA-02, Version 1.3.2.

[7] Protection Profile Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 (EAC2 PP), BSI-CC-PP-0086, Version 1.01.

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

[9] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), certified under the reference BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01.

[10] Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (BAC PP), certified under the reference BSI-CC-PP-0055-2009, Version 1.10, BSI-CC-PP-0055.

[11] Protection Profile Machine-Readable Electronic Document based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087-V2-MA-01, Version 2.0.3.

9 . 2 Developer documents

[12] ChipDoc 4.0 Applet User Guide Manual, NXP Semiconductors, Ref. 654214, Revision 1.4, date 27 December 2022.

[13] ChipDoc 4.0 SSCD Personalization Guide, NXP Semiconductors, Ref. 654412, Revision 1.2, date 14 October 2022.

[14] ChipDoc 4.0 ICAO Personalization Guide, NXP Semiconductors, Ref. 654311, Revision 1.1, date 19 October 2022.

[15] ChipDoc 4.0 Applet Release Note - Release Note for ChipDoc 4.0.1.4JxR Applet , NXP Semiconductors, Revision 1.1, date 3 November 2022.

[16] NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2), Security Target Lite, NXP Semiconductors, Rev. 1.4, 14 October 2022, BSI-DSZ-CC-1149-2022 with Maintenance certification report BSI-DSZ-CC-1149-2022-MA-1.

[17] JCOP 4.5 P71 Security Target Lite for JCOP 4.5 P71, NXP Semiconductors, Rev. 1.5, 27 October 2022, NSCIB CC-22-0313985 with Maintenance certification report NSCIB-CC-0313985-MA-1.

[18] JCOP 4.5 P71 User manual for JCOP 4.5 P71, User Guidance and Administrator Manual, NXP Semiconductors, Ref. 615217, Rev. 1.7, 13 October 2022..

9 . 3 Standards

[19] ETSI TS 119312, Technical Specification - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, v1.4.2, February 2022.

[20] FIPS PUB 180-4: Secure Hash Standard (SHS), August 2015.

[21] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

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

[23] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris Dworkin, National Institute of Standards and Technology, December 2001.

[24] NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, National Institute of Standards and Technology, May 2005.

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

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

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

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

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

[30] Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21. December 2016

[31] Technical Guideline TR-03111, Elliptic Curve Cryptography , Version 2.10, 01 June 2018

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

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

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

[35] GlobalPlatform Technology - Secure Channel Protocol '03', CSv2.3 Amendment D, ref GPC_SPE_014, v1.2

[36] GlobalPlatform Technology - Executable Load File Update, CSv2.3 Amendment H, ref GPC_SPE_120, v1.1

[37] GlobalPlatform Technology - Secure Element Management Service, CSv2.3 Amendment I, ref GPC_SPE_121, v1.1

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

10 Legal information

10.1 Definitions

Draft — A draft status on a document indicates that 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 in a draft version of a document and shall have no liability for the consequences of use of such information.

10.2 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 and its suppliers accept 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.

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.

Suitability for use in 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, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

10.3 Trademarks

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

NXP — wordmark and logo are trademarks of NXP B.V.

DESFire — is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

Tables

Figures

Contents

All information provided in this document is subject to legal disclaimers.

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

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

Date of release: 24 January 2023
Document identifier: CDv4_1_310390_STLite_CDv4_ICAO_EAC_PACE