Giesecke+Devrient

VERIDOS
IDENTITY SOLUTIONS
by Giesecke+Devrient
and Bundesdruckerei

# ePass Applet on Sm@rtCafé® Expert 8.0 C2

## Security Target Lite

Version 2.0/Status 09.10.2023

Author : G+D ePayments GmbH

Status : Final

Rating : Public

File : ePass Applet on SCE_8_0_C2_ASE_Lite.doc

# Contents

# 1 ST Introduction

This document is the Security Target Lite for the TOE ePass Applet on Sm@rtCafé® Expert 8.0 C2.

## 1.1 ST Reference

Title: Security Target Lite ePass Applet on Sm@rtCafé® Expert 8.0 C2
Reference: ASE_ePass Applet on Sm@rtCafé® Expert 8.0 C2

TOE Version: 1.0

Document Version Number: Version 2.0/Status 09.10.2023

Origin: Giesecke+Devrient ePayments GmbH

Author: G+D / stut

Compliant to: [PP_EAC], [PP_SAC] and [PP_BAC]

## 1.2 TOE Reference

TOE Reference: ePass Applet on Sm@rtCafé® Expert 8.0 C2

The TOE Name is ePass Applet on Sm@rtCafé® Expert 8.0 C2, Version 1.0

The TOE is a secure chip implementing an ePassport.

The TOE is subject to a composite certification based on Sm@rtCafé® Expert 8.0 C2 [SCE 8.0 ST]

HW-Part of TOE:

IFX SLC37GDA448/512 (Certificate: BSI-DSZ-CC-1107-V3-2022), [IFX_Cert], [IFX_ST].

### 1.2.1 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides general purpose and TOE description.

Section 3 contains the conformance claims for the TOE.

Section 4 contains the security problem definition.

Section 5 contains the security objectives for the TOE and its environment, including the security objectives rationale.

Section 6 contains the extended components definition.

Section 7 contains the security functional requirements, including the security requirements rationale.

Section 8 contains the TOE summary specification.

Section 9 contains references and abbreviations.

### 1.2.2 Typographic Conventions

- **This typeface** is used to highlight assignments, selections and refinements for SFRs completed by the ST author.
- **This typeface** used to highlight assignments and selections for SFRs defined in the PP.

### 1.2.3 Change History

| Version | Date | Changes | Responsible |
|---|---|---|---|
| 2.0 | 09.10.23 | Final version | stut |

### 1.2.4 Tables



### 1.2.5 Application notes of the PP

When applicable the application notes of the PP are discussed in Application Note (of the ST author).

# 2 TOE Overview

### 2.1.1 TOE Definition

The Target of Evaluation (TOE) described in this ST is an electronic passport representing a smart card implementing [ICAO_9303_10], [ICAO_9303_11], [TR-03110_1] and [TR-03110_3].

This smart card / passport provides the following application:

- the travel document containing the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols (incl. PACE/BAC passwords); this application is intended to be used by governmental organisations as a machine readable travel document (MRTD).

The TOE comprises of

- the circuitry of the travel document's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the ePassport application (as the only application on the IC) and
- the associated guidance documentation.

After mask development under the responsibility of G+D, the cards are delivered in an initialized state to the personalizer.

### 2.1.2 TOE Operational Usage

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods (see [ICAO_9303_1]) in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip. The authentication of the traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

### 2.1.3 TOE Major Security Features

The following TOE security features are the most significant for its operational use:

- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the connected terminal supporting the protocols BAC, SAC(PACE) as per [ICAO_9303_11] and EAC as per [TR-03110_1]
- Averting of inconspicuous tracing of the travel document as per [TR-03110_1]
- Self-protection of the TOE security functionality and the data stored inside as per [TR-03110_1]
- Means to check authenticity of the terminal, Terminal Authentication as per [TR-03110_1]
- Means to prove authenticity of the chip by means of Active Authentication or Chip Authentication as per [TR-03110_1]
- Chip authentication followed by terminal authentication used as a precondition to provide access to biometric data known as EAC, as per [TR-03110_1]

## 2.2 TOE Description

### 2.2.1 Component Overview

The TOE is a pure contactless smart card with Java Card OS and ePassport application. This is based on the requirements from the ICAO for machine readable travel documents, i.e. [ICAO_9303_10], [ICAO_9303_11], [TR-03110_1] and [TR-03110_3].

The TOE operating system does not include other applications than the ePassport application.

The OS platform called Sm@rtCafé® Expert 8.0 C2 [SCE 8.0 ST] is a Java Card OS and offers services for:

- The standard Java Card features like API, the Java Card Runtime Environment and the Java Card Virtual Machine
- Proprietary PACE API providing special countermeasures against side channel leakage
- GP for content management
- Crypto operation via the contactless interface and contact interface
- Communication via the contactless interface and contact interface.

It is certified in Common Criteria under the Certificate NSCIB CC-22-0289060 [SCE 8.0 Cert].

ePass Applet on Sm@rtCafé® Expert 8.0 C2 is a Java Card applet which provides the functions of the electronic Passport as per [ICAO_9303_10], [ICAO_9303_11], [TR-03110_1] and [TR-03110_3].

The installation of ePass Applet on Sm@rtCafé® Expert 8.0 C2 is done by the initializer (G+D/Veridos).

The applet uses the services of the Java Card OS described above. It manages the various stages of the product's lifecycle once the application is onto the hardware up to its end of life. The application implements the protocols:

- BAC
- PACE
- EAC
- AA

It does not implement any cryptographic primitives, as these are provided by the underlying Java Card OS. Further it manages file access control and authentication failure handling. Also the application controls the secure messaging including error handling using the Java Card OS Crypto services, which subsequently relies on the features of the underlying hardware providing high integrity and side channel protection. The claims in terms of SFRs in this ST target the ePass Applet on Sm@rtCafé® Expert 8.0 C2.

The product containing the TOE is based on and designed to be compliant to the following specifications:

- The Java Card specification (see: [JCVM31], [JCRE301], [JCAPI304], [JCAPI31]);

These industry standards are aimed at defining a framework with which Applications can be developed, managed and used on a Java Card Platform Embedded Software like case Sm@rtCafé® Expert 8.0 C2 [SCE 8.0 ST].

Note that after Sm@rtCafé® Expert 8.0 C2 [SCE 8.0 ST] is initialized and the TOE is delivered to the personalizer no GP commands for content management are available so that the customer will not be able to load and install 3rd party applications.

The physical scope of the TOE is:

- the TOE documentation (pdf documents, that are to be delivered PGP-encrypted electronically or per CD or delivered in a printed version):
  - Main Guidance [UGMain]
  - Preparative Guidance, [UGPre]
  - Operative Guidance, [UGOpe]
  - Personalization Concept [UGPerso]
  - Usage Phase Commands [UGUsage]
  - Operative Guidance of the underlying Sm@rtCafé® Expert Java Card Plattform, [UGOpe-SCE]
- the ePass Applet on the Java Card OS platform Sm@rtCafé® Expert 8.0 C2 ([SCE 8.0 ST]) on a Infineon chip (IFX SLC37GDA448/512 (Certificate: BSI-DSZ-CC-1107-V3-2022), [IFX_Cert], [IFX_ST]) as a pure contactless card (sent per postal service in a sealed way)

## 2.3 TOE life cycle

The [PP_EAC], [PP_SAC] and [PP_BAC] define the lifecycle phases for the TOE as follows:

**1. Development**

**- Step 1:** Development of hardware and IC dedicated software (firmware)

**- Step 2:** Development of IC embedded software

**2. Manufacturing**

**- Step 3:** manufacturing of IC and IC dedicated software. As the TOE does not provide any user ROM, manufacturing of IC embedded software parts in ROM are not relevant here.

**- Step 4 (optional):** Combination of IC with contactless interface of the travel document

**- Step 5 (Prepersonalization):** loading on the device the executable Java Card OS image. Loading of the application JC package containing the TOE code, eDL and eID code. Then the ePass Applet is initialized on Sm@rtCafé® Expert 8.0 C2. After this step the TOE is delivered to the customer.

**3. Personalisation of Travel Document**

**- Step 6:** this step is performed by the customer. The customer receives from Infineon or G+D/Veridos the TOE composed of the following components:

- The underlying hardware

- The initialized ePass Applet on Sm@rtCafé® Expert 8.0 C2

The customer then performs the personalisation with biometric data and configuration of the TSF if necessary.

**4. Operational Use**

**- Step 7:** once the personalization of the product is finished, the Java Card OS Sm@rtCafé® Expert 8.0 C2 [SCE 8.0 ST] is switched to its proprietary privacy mode usage of the TOE by the personalizer.

Privacy mode switches identification commands from Sm@rtCafé® Expert 8.0 C2 OS and ePass Applet to disallow tracking of the end user.

Only ePass Applet commands for the operational phase are allowed in this mode.

# 3 Conformance Claims

## 3.1 CC conformance claims

This ST claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, version 3.1, revision 5, CCMB-2017-04-001 [CC1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, April 2017, version 3.1, revision 5, CCMB-2017-04-002 [CC2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, April 2017, version 3.1, revision 5, CCMB-2017-04-003 [CC3].

as follows

- Part 2 extended,
- Part 3 conformant.

## 3.2 PP claim

This ST claims *strict* conformance

- to [PP_BAC], if a BIS chooses BAC as authentication method
- to [PP_SAC], if a BIS chooses PACE as authentication method
- to [PP_EAC], if a EIS choses PACE as authentication method and additionally uses Extended Access Control, which consists of two parts (i) the Chip Authentication Protocol Version 1 (v.1) and (ii) the Terminal Authentication Protocol Version 1 (v.1) as defined in [TR-03110_1].

## 3.3 Package claim

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5 in case PACE is used and EAC is not used and conform to [PP_SAC].

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5 in case PACE and EAC are used and conform to [PP_EAC].

The assurance level for the TOE is EAL4 augmented with the components ALC_DVS.2 and ATE_DPT.2 in case BAC is chosen as authentication method whereby conformancy to [PP_BAC] is claimed.

## 3.4 Statement of Compatibility concerning Composite Security Target

### 3.4.1 Assessment of the Platform TSFs

The following table lists all Security Functionalities of the underlying Platform ST [SCE 8.0 ST] and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

| Platform TSF-group | Correspondence in this ST | References/Remarks |
|---|---|---|
| SF.TRANSACTION | No correspondence, internal Java card mechanisms. | This security function provides atomic transactions according to the Java Card Transaction and Atomicitymechanism with commit and roll-back capability for updating persistent data in flash memory. |
| SF.ACCESS_CONTROL | No correspondence, internal Java card mechanisms. | This security function provides control for the TOE. It is in charge of the FIREWALL access control SFP and the JCVM information flow control SFP. Itenforces applet isolation located in different packages and controls the access to global data containers shared by all applet instances. |
| SF.CRYPTO | SF_Authentication, SF_KeyManagement | This security function controls all the operations related to the cryptographic key management and cryptographic operations. |
| SF.INTEGRITY | SF_TSFProtection | This security function provides a means to demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. |

| | | |
|---|---|---|
| SF.SECURITY | SF_TSFProtection | This security function detects physical tampering of the TSF with sensors and then a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. |
| SF.APPLET | No correspondence, internal Java card mechanisms. | This security function ensures the secure loading of a package or installing of an applet and the secure deletion of applets and/or packages. |
| SF.CARRIER | No correspondence, TOE cannot download applications on the card. | This security function ensures secure downloading of applications on the card. |

**Table 1 Relevant platform TSF-groups and their correspondence**

### 3.4.2 Assessment of the Platform SFRs

The following table provides an assessment of all Platform SFRs. The Platform SFRs are listed in the order used within the security target of the platform [SCE 8.0 ST].

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| CoreG_LC Security Functional Requirements (chapter 8.1.1 in platform ST) | | |
| Firewall Policy (chapter 8.1.1.1 in platform ST) | | |
| FDP_ACC.2/FIREWALL<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall. The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST. |
| FDP_ACF.1/FIREWALL<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST. |
| FDP_IFC.1/JCVM<br>IP_SFR | No correspondence | Out of scope (internal Java Virtual Machine). No contradiction to this ST. |
| FDP_IFF.1/JCVM<br>IP_SFR | No correspondence | Out of scope (internal Java Virtual Machine). No contradiction to this ST. |
| FDP_RIP.1<br>(FDP_RIP.1/OBJECTS<br>FDP_RIP.1/APDU<br>FDP_RIP.1/bArray<br>FDP_RIP.1/KEYS<br>FDP_RIP.1/TRANSIENT | No correspondence. | Out of scope (internal Java Card Firewall). No contradiction to this ST. |

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FDP_RIP.1/ADEL<br>FDP_RIP.1/ODEL<br>FDP_RIP.1/ABORT)<br>All IP_SFRs | | |
| FMT_MSA.1/JCRE<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). No contradiction to this ST. |
| FMT_MSA.1/JCVM<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). No contradiction to this ST. |
| FMT_MSA.2/FIREWALL-JCVM<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST. |
| FMT_MSA.3/FIREWALL<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST. |
| FMT_MSA.3/JCVM<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). No contradiction to this ST. |
| FMT_SMF.1<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). No contradiction to this ST. |
| FMT_SMR.1<br>IP_SFR | No correspondence | Out of scope (internal Java Card Firewall). No contradiction to this ST. |
| Application Programming Interface (chapter 8.1.1.2 in platform ST) | | |
| FCS_CKM.1<br>(FCS_CKM.1.1/RSA,<br>FCS_CKM.1.1/ECC,<br>FCS_CKM.1.1/3DES,<br>FCS_CKM.1.1/AES)<br>All IP_SFRs | No crrespondence. | Out of scope. The TOE uses the specific Document Basic Access Key Derivation Algorithm. There are no contradictions to this ST. |
| FCS_CKM.2<br>IP_SFR | No correspondence | Out of scope (managed within Java Card OS). No contradiction to this ST. |
| FCS_CKM.3<br>IP_SFR | No correspondence | Out of scope (managed within Java Card OS). No contradiction to this ST. |
| FCS_CKM.4<br>RP_SFR-SERV | FCS_CKM.4 | The requirements are compatible (physically overwriting the keys, physically overwriting the keys with zeros). Thus, all internal Java Card key objects fulfill the requirement of this ST. There are no contradictions. |
| FCS_COP.1<br>(FCS_COP.1.1/RSA-CRT- | FCS_COP.1/SHA,<br>FCS_COP.1/ENC, | The requirements of this ST are equivalent to a subset of the platform |

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| SIGN, FCS_COP.1.1/RSA-SIGN, FCS_COP.1.1/RSA-VERI, FCS_COP.1.1/MAC-DES, FCS_COP.1.1/MAC-AES, FCS_COP.1.1/CMAC-AES, FCS_COP.1.1/3DES, FCS_COP.1.1/AES, FCS_COP.1.1/RSA-DEC, FCS_COP.1.1/RSA-CRT-DEC, FCS_COP.1.1/RSA-ENC, FCS_COP.1.1/ECDSA-SIGN, FCS_COP.1.1/ECDSA-VERI, FCS_COP.1.1/HASH)<br>All RP_SFR-SERV | FCS_COP.1/AUTH,<br>FCS_COP.1/MAC<br>FCS_COP.1/PACE_ENC<br>FCS_COP.1/PACE_MAC<br>V FCS_COP.1/CA_ENC<br>FCS_COP.1/CA_MAC<br>FCS_COP.1/SIG_VER<br>FCS_COP.1/SIG_GEN | requirements: FCS_COP.1/SHA of this ST corresponds to the platform SFR FCS_COP.1.1/HASH; FCS_COP.1/ENC corresponds to the platform SFR FCS_COP.1.1/3DES; FCS_COP.1/AUTH corresponds to the platform SFR FCS_COP.1.1/AES; FCS_COP.1/MAC corresponds to the platform SFR FCS_COP.1.1/MAC-DES.<br>No contradictions to this ST. |
| FCS_RNG.1<br>RP_SFR-SERV | FCS_RND.1 | In this ST, random numbers according to AIS20 class DRG.3 are required. The platform generates random numbers with a defined quality metric (DRG.3) that can be used directly. |
| FDP_RIP.1/ABORT<br>IP_SFR | No correspondence. | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_RIP.1/APDU<br>IP_SFR | No correspondence. | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_RIP.1/bArray<br>IP_SFR | No correspondence. | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_RIP.1/KEYS<br>IP_SFR | No correspondence. | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_RIP.1/TRANSIENT<br>IP_SFR | No correspondence. | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_ROL.1/FIREWALL<br>IP_SFR | No correspondence. | Out of scope (internal Java Card Firewall). The resulting requirements for applets are reflected in the User Guidance of the TOE. No contradiction to this ST. |
| Card Security Management (chapter 8.1.1.3 in platform ST) | | |
| FAU_ARP.1<br>RP_SFR-MECH | FPT_FLS.1, FPT_FLS.1/BAC<br>FPT_PHP.3 | Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. Internal counter for security violations complement Java Card OS mechanisms- No contradiction to this ST. |

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FDP_SDI.2<br>RP_SFR-MECH | FPT_FLS.1, FPT_FLS.1/BAC<br>FPT_PHP.3 | Not directly corresponding, but platform SFR is basis of fulfillment of FPT_FLS.1 and FPT_PHP.3. No con- tradiction to this ST. |
| FPR_UNO.1<br>RP_SFR-MECH | FPT_EMSEC.1<br>FPT_EMS.1<br>FPT_EMS.1/EAC | Not directly corresponding, but relevant for the fullfillment of FPT_EMSEC.1. No contradiction to this ST. |
| FPT_FLS.1<br>RP_SFR-SERV | FPT_FLS.1, FPT_FLS.1/BAC | The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction tothis ST. |
| FPT_TDC.1<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FPT_TST.1<br>RP_SFR-SERV | FPT_TST.1 | Self-testing is provided by the Java Card platform during initial start-up. |
| AID Management (chapter 8.1.1.4 in platform ST) | | |
| FIA_ATD.1/AID<br>IP_SFR | No correspondence. | Out of scope (internal Java Card fun tionality). No contradiction to this ST. |
| FIA_UID.2/AID<br>IP_SFR | No correspondence | Out of scope (internal Java Card fun tionality). No contradiction to this ST. |
| FIA_USB.1/AID<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_MTD.1/JCRE<br>IP_SFR | No correspondence | Out of scope (internal Java Card fun tionality). No contradiction to this ST. |
| FMT_MTD.3/JCRE<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| INSTG Security Functional Requirements (chapter 8.1.2 in platform ST)<br>This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime. | | |
| FDP_ITC.2/Installer<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_SMR.1/Installer<br>IP_SFR | No correspondence | Out of scope (internal Java Card func tionality). No contradiction to this ST. |
| FPT_FLS.1/Installer<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FPT_RCV.3/Installer<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| ADELG Security Functional Requirements (chapter 8.1.3 in platform ST)<br>This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime. | | |
| FDP_ACC.2/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_ACF.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_RIP.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_MSA.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_MSA.3/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_SMF.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_SMR.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FPT_FLS.1/ADEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| ODELG Security Functional Requirements (chapter 8.1.4 in platform ST)<br>The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method. | | |
| FDP_RIP.1/ODEL<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FPT_FLS.1/ODEL<br>RP_SFR-SERV | FPT_FLS.1, FPT_FLS.1/BAC | The fulfillment of the platform SFR is part of the basis of the fulfillment of the SFR of this ST. Internal countermeasures for detecting security violations complement Java Card OS mechanisms. No contradiction tothis ST. |
| CARG Security Functional Requirements (chapter 8.1.5 in platform ST)<br>This group includes requirements for preventing the installation of packages that has not been bytecode verified, or that has been modified after bytecode verification. | | |
| FCO_NRO.2/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |

| Platform SFR | Correspondence in this ST | References/Remarks |
|---|---|---|
| FDP_IFC.2/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_IFF.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FDP_UIT.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FIA_UID.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_MSA.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_MSA.3/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_SMF.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FMT_SMR.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| FTP_ITC.1/CM<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| CMGR Security Functional Requirements (chapter 8.1.6 in platform ST)<br>In the PP of the Java Card certification [JCSPP], objectives for Card Management were objectives for the environment. Since the card manager has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST. | | |
| FTP_ITC.1/CMGR<br>IP_SFR | No correspondence | Out of scope (internal Java Card functionality). No contradiction to this ST. |
| SCPG Security Functional Requirements (chapter 8.1.7 in platform ST)<br>In the PP of the Java Card certification [JCSPP], objectives for the smart card platform are objectives for the environment. Since the smart card platform has been defined to be part of the TOE, they were transformed into objectives for the TOE and are covered by SFRs in the platform ST. | | |
| FPT_PHP.3<br>RP_SFR-SERV | FPT_PHP.3<br>FPT_EMSEC.1<br>FPT_EMS.1<br>FPT_EMS.1/EAC | The fulfillment oft he SFR in this ST is based on the platform SFR (together with additional countermeasures). |

### 3.4.3 Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

| Platform Objective | Correspondence in this ST | References/Remarks |
|---|---|---|

| Platform Objective | Correspondence in this ST | References/Remarks |
|---|---|---|
| O.SID | No correspondence | Out of scope. No contradiction tothis ST. |
| O.FIREWALL | No correspondence | Out of scope. No contradiction tothis ST. |
| O.GLOBAL_ARRAYS_CONFID | OT.Data-Confidentiality | No contradiction to this ST. |
| O.GLOBAL_ARRAYS_INTEG | OT.Data-Integrity | No contradiction to this ST. |
| O.ARRAY_VIEWS_CONFID | No correspondence | Out of scope. No contradiction to this ST. |
| O.ARRAY_VIEWS_INTEG | No correspondence | Out of scope. No contradiction to this ST. |
| O.NATIVE | No correspondence | Out of scope. No contradiction to this ST. |
| O.OPERATE | No correspondence | Out of scope. No contradiction to this ST. |
| O.REALLOCATION | No correspondence | Out of scope. No contradiction to this ST. |
| O.RESOURCES | No correspondence | Out of scope. No contradiction to this ST. |
| O.ALARM | No correspondence | Out of scope. No contradiction to this ST. |
| O.CIPHER | No correspondence | Indirectly relevant for the correct function of the TOE of this ST, but no corresponding objectives for the TOE of this ST. No contradictions. |
| O.RNG | No correspondence | Indirectly relevant for the correct function of the TOE of this ST, but no corresponding objectives for the TOE of this ST. No contradictions. |
| O.KEY-MNGT | No correspondence | Out of scope. No contradiction to this ST. |
| O.PIN-MNGT | No correspondence | Out of scope. No contradiction to this ST. |
| O.TRANSACTION | No correspondence | Out of scope. No contradiction to this ST. |
| O.OBJ-DELETION | No correspondence | Out of scope. No contradiction to this ST. |
| O.DELETION | No correspondence | Out of scope. No contradiction to this ST. |
| O.LOAD | No correspondence | Out of scope. No contradiction to this ST. |
| O.INSTALL | No correspondence | Out of scope. No contradiction to this ST. |
| O.CARD-MANAGEMENT | No correspondence | Out of scope. No contradiction to this ST. |
| OT.SCP.IC | OT.Prot_Phys-Tamper | The objectives are related. No contradiction to this ST. |
| OT.SCP.RECOVERY | OT.Prot_Malfunction | The objectives are related. No contradiction to this ST. |
| O.SCP.SUPPORT | No correspondence | Out of scope. No contradiction to this |

| Platform Objective | Correspondence in this ST | References/Remarks |
|---|---|---|
| | | ST. |

### 3.4.4 Assessment of Platform Threats

The following table provides an assessment of all relevant Platform threats.

| Platform Threat | Correspondence in this ST | References/Remarks |
|---|---|---|
| T.CONFID-APPLI-DATA | No correspondence | Out of scope. No contradiction to this ST. |
| T.CONFID-JCS-CODE | No correspondence | Out of scope. No contradiction to this ST. |
| T.CONFID-JCS-DATA | T.Information_Leakage | No contradiction to this ST. |
| T.INTEG-APPLI-CODE | No correspondence | Out of scope. No contradiction to this ST. |
| T.INTEG-APPLI-CODE.LOAD | No correspondence | Out of scope. No contradiction to this ST. |
| T.INTEG-APPLI-DATA | T.Forgery | No contradiction to this ST. |
| T.INTEG-APPLI-DATA.LOAD | No correspondence | Out of scope. No contradiction to this ST. |
| T.INTEG-JCS-CODE | No correspondence | Out of scope. No contradiction to this ST. |
| T.INTEG-JCS-DATA | No correspondence | Out of scope. No contradiction to this ST. |
| T.SID.1 | No correspondence | Out of scope. No contradiction to this ST. |
| T.SID.2 | No correspondence | Out of scope. No contradiction to this ST. |
| T.EXE-CODE.1 | No correspondence | Out of scope. No contradiction to this ST. |
| T.EXE-CODE.2 | No correspondence | Out of scope. No contradiction to this ST. |
| T.NATIVE | No correspondence | Out of scope. No contradiction to this ST. |
| T.RESOURCES | No correspondence | Out of scope. No contradiction to this ST. |
| T.DELETION | No correspondence | Out of scope. No contradiction to this ST. |
| T.SECURE_DELETION | No correspondence | Out of scope. No contradiction to this ST. |
| T.INSTALL | No correspondence | Out of scope. No contradiction to this ST. |
| T.OBJ-DELETION | No correspondence | Out of scope. No contradiction to this ST. |

| Platform Threat | Correspondence in this ST | References/Remarks |
|---|---|---|
| T.PHYSICAL | T.Phys-Tamper | No contradiction to this ST. |

### 3.4.5 Assessment of Platform Organisational Security Policies

The platform ST contains the Organisational Security Policy "OSP.VERIFICATION" that focuses on the integrity of loaded applets. This policy does not contradict to the policies of this ST.

### 3.4.6 Assessment of Platform Operational Environment

#### 3.4.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

| Platform Assumption | Relevance for Composite ST |
|---|---|
| A.CAP_FILE | Not relevant.<br>A.APPLET states that applets loaded post-issuance do not contain native methods.<br>This Composite TOE does not support applet loading post-issuance. |
| A.VERIFICATION | Not relevant.<br>This assumption targets the applet code verification.<br>This Composite TOE does not support applet loading post-issuance. |

#### 3.4.6.2 Assessment of Platform Objectives for the Operational Environment

There are the following Platform Objectives for the Operational Environment that have to be considered.

| Platform Objective for the Environment | Relevance for Composite ST |
|---|---|
| OE.CAP_FILE | Not relevant.<br>The platform objective for the environment states that applets loaded post-issuance do not contain native methods.<br>This Composite TOE does not support applet loading post-issuance. |
| OE.VERIFICATION | Not relevant.<br>The platform objective for the environment targets the applet code verification.<br>This Composite TOE does not support applet loading post-issuance. |
| OE.CODE-EVIDENCE | Not relevant.<br>The platform objective for the environment focusses on application code loaded pre-issuance or post-issuance.<br>This Composite TOE does not support applet loading post-issuance.<br>This Composite TOE does not have other applet besides the TOE. |

### 3.4.7 Assessment of Platform assurance requirements

The Platform-ST requires EAL 6 augmented with ALC_FLR.1.

This ST requires EAL 5 augmented with the components ALC_DVS.2 and AVA_VAN.5.

Therefore, the assurance requirements for this TOE are a subset of the assurance requirements of the Platform TOE.

# 4 Security Problem Definition

All assets, subjects and external entities, threats, organisational security policies and assumptions from [PP_EAC], [PP_SAC] and [PP_BAC] section 3 “Security Problem Definition” are applicable for this TOE.

# 5 Security objectives

Here follows a concise description of the security objectives applying to this ST followed by a the security objective rationale.

## 5.1 Security Objectives defined in the claimed PPs

All Security Objectives provided by the TOE or by the operational environment as well as the security objectives rationale from the claimed PPs [PP_EAC], [PP_SAC] and [PP_BAC] section 4 “Security Objectives” are applicable for this TOE.

## 5.2 Security Objectives defined in this ST

The following security objectives are defined additionally in this ST to formally express the extra features of the TOE not present in the claimed PPs:

**OT.Active_Auth Travel document’s chip authenticity**

The TOE shall support the Basic 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 Active Authentication as defined in [ICAO_9303_1]. The authenticity proof provided by travel document’s chip shall be protected against attacks with high attack potential.

**OE.Active_Auth_Key_MRTD MRTD Active Authentication Key**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD’s Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD’s chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

## 5.3 Security Objective Rationale

The Security Objective Rationale from the claimed PPs [PP_EAC], [PP_SAC] and [PP_BAC] stays the same here.

The additionally defined security objectives in this ST **OT.Active_Auth** and **OE.Active_Auth_Key_MRTD** above counters the threat **T.Counterfeit** (threat defined in [PP_EAC].

# 6 Extended Components Definition

[PP_EAC], [PP_SAC] and [PP_BAC] respective sections 5 “Extended Components Definition” are applicable for this TOE.

# 7 Security Requirements

## 7.1 TOE Security functional requirements

The security functional requirements (SFR) for this TOE are defined in this chapter.

This ST covers the three PPs [PP_SAC], [PP_EAC] and [PP_BAC] each two of which have a non empty intersection of SFRs. In the rest of this section we provide a classification of the SFRs of these PPs depending on where these SFRs are declared and if they need a refinement here in this ST.

Table 1 lists all SFRs appearing both in [PP_SAC] and [PP_BAC].

Table 2 lists all SFRs declared in [PP_SAC].

Table 3 lists all SFRs specific to [PP_BAC]. Note that some of the SFRs appear in both [PP_SAC] and [PP_BAC] with same name but different content. In such cases the SFR is iterated with either the extension …/BAC or …/PACE.

Table 4 lists all SFRs specific to [PP_EAC]. Note that [PP_EAC] is an extension of [PP_SAC], therefore all SFRs of [PP_SAC] are SFRs in [PP_EAC], i.e. the SFRs listed in Table 3 and Table 4 are also SFRs of [PP_EAC].

Table 5 lists the SFRs introduced in this ST which are related to the Active Authentication mechanism supported by the TOE.

| **TOE SFRs equivalent from both [PP_SAC] and [PP_BAC]** |
|---|
| FCS_CKM.4 |
| FCS_RND.1 |
| FMT_MTD.1/INI_ENA |
| FPT_TST.1 |
| FPT_PHP.3 |

**Table 2 TOE SFRs equivalent from both [PP_SAC] and [PP_BAC]**

| **TOE SFRs equivalent from [PP_SAC]** |
|---|
| FCS_CKM.1/DH_PACE |
| FCS_COP.1/PACE_ENC |
| FCS_COP.1/PACE_MAC |
| FIA_AFL.1/PACE |
| FIA_UID.1/PACE |
| FIA_UAU.1/PACE |
| FIA_UAU.4/PACE |
| FIA_UAU.5/PACE |
| FIA_UAU.6/PACE |

| |
|---|
| FDP_ACC.1/TRM |
| FDP_ACF.1/TRM |
| FDP_UCT.1/TRM |
| FDP_UIT.1/TRM |
| FDP_RIP.1<br>FTP_ITC.1/PACE |
| FAU_SAS.1 |
| FMT_SMF.1 |
| FMT_SMR.1/PACE |
| FMT_MTD.1/INI_DIS |
| FMT_MTD.1/KEY_READ |
| FMT_MTD.1/PA |
| FPT_EMS.1 |
| FPT_FLS.1 |

**Table 3 TOE SFRs equivalent from [PP_SAC]**

| TOE SFRs equivalent from [PP_BAC] |
|---|
| FCS_CKM.1 |
| FCS_COP.1/SHA |
| FCS_COP.1/ENC |
| FCS_COP.1/AUTH |
| FCS_COP.1/MAC |
| FIA_UID.1 |
| FIA_UAU.1 |
| FIA_UAU.4 |
| FIA_UAU.5 |
| FIA_UAU.6 |
| FIA_AFL.1 |
| FDP_ACC.1 |
| FDP_ACF.1 |
| FDP_UCT.1 |
| FDP_UIT.1 |
| FAU_SAS.1/BAC |
| FMT_SMF.1/BAC |
| FMT_LIM.1/BAC |
| FMT_LIM.2/BAC |
| FMT_MTD.1/INI_DIS/BAC |
| FMT_MTD.1/KEY_WRITE |

| |
|---|
| FMT_MTD.1/KEY_READ_BAC |
| FMT_SMR.1 |
| FPT_EMSEC.1 |
| FPT_FLS.1/BAC |

**Table 4 TOE SFRs equivalent from [PP_BAC]**

| TOE SFRs equivalent from [PP_EAC] |
|---|
| FCS_CKM.1/CA |
| FCS_COP.1/CA_ENC |
| FCS_COP.1/SIG_VER |
| FCS_COP.1/CA_MAC |
| FIA_UID.1/PACE_EAC |
| FIA_UAU.1/PACE_EAC |
| FIA_UAU.4/PACE_EAC |
| FIA_UAU.5/PACE_EAC |
| FIA_UAU.6/EAC |
| FIA_API.1 |
| FDP_ACC.1/TRM |
| FMT_SMR.1/PACE_EAC |
| FMT_LIM.1 |
| FMT_LIM.2 |
| FMT_MTD.1/CVCA_INI |
| FMT_MTD.1/CVCA_UPD |
| FMT_MTD.1/DATE |
| FMT_MTD.1/CAPK |
| FMT_MTD.1/KEY_READ_EAC |
| FMT_MTD.3 |
| FPT_EMS.1/EAC |

**Table 5 TOE SFRs equivalent from [PP_EAC]**

| TOE SFRs introduced in this ST |
|---|
| FIA_API.1/AA |

| |
|---|
| FMT_MTD.1/AAPK |
| FCS_COP.1/SIG_GEN |

**Table 6 TOE SFRs introduced in this ST**

## 7.1.1 Common SFRs from [PP_BAC] and [PP_SAC]

### 7.1.1.1 Class FCS: Cryptographic Support

#### FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: fulfilled by
FCS_CKM.1/DH_PACE and FCS_CKM.1/CA

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key value with zero values[1] that meets the following: none[2].

**Application Note 1 (of the ST author):** The TOE destroys any session keys after detection of an error in verification of the MAC of a received command. The PACE Session Keys are destroyed after generation of the Chip Authentication Session Key (i.e. successfully performing the Chip Authentication) and changing the secure messaging to the Chip Authentication Session Keys. The TOE clears the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

#### Random Number Generation (FCS_RND.1)

The TOE meets the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

#### FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

[1] [assignment: *cryptographic key destruction method*]

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

**FCS_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet DRG3 according to AIS20 [AIS20][3].

**Application Note 2 (of the ST author):** The TOE generates random numbers used for the authentication protocols e. g. as required by FIA_UAU.4/**PACE**.

#### 7.1.1.2 Class FMT Security Management

**FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation Data**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

**FMT_MTD.1.1/INI_ENA** The TSF shall restrict the ability to write [4] the Initialisation Data and Pre-personalisation Data[5] to the Manufacturer. [6]

#### 7.1.1.3 Class FPT Protection of the Security Functions

**FPT_TST.1 TSF testing**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_TST.1.1** The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition[7] Reset of the TOE[8] to demonstrate the correct operation of the TSF[9].

**FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[10].

**FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[11].

---

[3] [assignment: *a defined quality metric*]

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

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

[6] [assignment: *the authorised identified roles*]

[7] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*]

[8] [assignment: *conditions under which self test should occur*]

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

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

### FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_PHP.3.1** The TSF shall resist physical manipulation and physical probing [12] to the TSF [13] by responding automatically such that the SFRs are always enforced.

**Application Note 3:** The TOE implements appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

## 7.1.2 SFRs specifically from [PP_SAC]

### FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES/3DES

Hierarchical to: No other components.

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

**FCS_COP.1.1/PACE_ENC** The TSF shall perform secure messaging – encryption and decryption[14] in accordance with a specified cryptographic algorithm AES and 3DES[15] in CBC mode[16] and cryptographic key sizes 112, 128, 192 and 256[17] [18] bit [19] that meet the following: compliant to [ICAO_9303_1][20].

---

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

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

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

[14] [assignment: *list of cryptographic operations*]

[15] [selection: *AES, 3DES*]

[16] [assignment: *cryptographic algorithm*]

[17] For 3DES 112 bit cryptographic key size, for AES 128, 192 and 256 bit cryptographic key size

[18] [selection: *128, 192, 256*]

[19] [assignment: *cryptographic key sizes*]

**Application Note 4:** TOE implements the cryptographic primitives (i.e. Triple-DES and AES) for secure messaging with encryption of the transmitted data and encrypting the nonce in the first step of PACE. The keys are agreed between the TOE and the terminal as part of the PACE protocol according to FCS_CKM.1/DH_PACE.

**FCS_COP.1/PACE_MAC Cryptographic operation – MAC**

Hierarchical to: No other components.

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

**FCS_COP.1.1/PACE_MAC** The TSF shall perform secure messaging – message authentication code[21] in accordance with a specified cryptographic algorithm CMAC and Retail-MAC[22] [23] [24] and cryptographic key sizes 112, 128, 192 and 256[25] [26] bit [27] that meet the following: compliant to [ICAO_9303_1][28].

**Application Note 5 (of the ST author):** The TOE to implements the cryptographic primitives (i.e. CMAC and Retail-MAC) for secure messaging with message authentication code over transmitted data. The keys are agreed between the TOE and the terminal as part of the PACE protocol according to FCS_CKM.1/DH_PACE

### 7.1.2.1 FCS: Cryptographic Support

**FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman for PACE session keys**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

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

[21] [assignment: *list of cryptographic operations*]

[22] For AES CMAC is used as MAC mechanism, for 3DES Retail-MAC is used as MAC mechanism

[23] [selection: *CMAC, Retail-MAC*]

[24] [assignment: *cryptographic algorithm*]

[25] For Retail-MAC 112 bit cryptographic key size, for CMAC 128, 192 and 256 bit cryptographic key size

[26] [selection: *112, 128, 192, 256*]

[27] [assignment: *cryptographic key sizes*]

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

FCS_COP.1 Cryptographic operation]: not fulfilled, but justified. Justification: A Diffie-Hellman key agreement is used in order to avoid key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

**FCS_CKM.1.1/DH_PACE** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [TR-3111][29,30] and specified cryptographic key sizes 112 bits[31], 128 bits, 192 bits and 256 bits[32,33] that meet the following: [ICAO_SAC][34].

**Application Note 6:** The TOE generates a shared secret value with the terminal during PACE Protocol, see [ICAO_SAC]. This protcol is based on the ECDH compliant to TR-03111 [TR-3111] (i.e. the elliptic curve cryptographic algorithm, ECKA, cf. [ICAO_SAC] and [TR-3111] for details). The shared secret value is used to derive session keys for message encryption and message authentication according to [ICAO_SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

**Application Note 7:** FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO_SAC].

#### 7.1.2.2 Class FIA Identification and Authentication

**FIA_AFL.1/PACE Authentication failure handling – PACE authentication using nonblocking authorisation data**

Hierarchical to: No other components.

Dependencies: UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

**FIA_AFL.1.1/PACE** The TSF shall detect when 15[35] [36] unsuccessful authentication attempts occurs related to authentication attempts using the PACE password as shared password[37].

[29] [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [TR-3111]]*

[30] [assignment: *cryptographic key generation algorithm*]

[31] Cryptographic key size of 2-key Triple-DES session keys

[32] Cryptographic key sizes of AES session keys

[33] [assignment: *cryptographic key sizes*]

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

[35] [assignment: *positive integer number*]

[36] [selection: [*assignment: positive integer number*], *an administrator configurable positive integer within* [assignment: *range of acceptable values*]]

[37] [assignment: *list of authentication events*]

**FIA_AFL.1.2/PACE** When the defined number of unsuccessful authentication attempts has been met[38], the TSF shall delay the PACE authentication after 6 unsuccessful authentication attempts[39].

**Application Note 8**: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [ICAO_SAC]) or for an arbitrary subset of them or may also separately be defined for each datum in question.Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy52, the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack53 requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP.One of some opportunities for performing this operation might be '*consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords*'.

### FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UID.1.1/PACE** The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO_SAC]
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. none [40]

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

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

**Application Note 9**: User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).

### FIA_UAU.1/PACE Timing of authentication

[38] [selection: met ,surpassed]

[39] [assignment: list of actions]

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE

**FIA_UAU.1.1/PACE** The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO_SAC],
3. to read the Initialisation Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. none[41]

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

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

**Application Note 10**: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).
If PACE was successfully performed, secure messaging is started using the derived PACE Session Keys, cf. FTP_ITC.1/PACE.

### FIA_UAU.4/PACE Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. PACE Protocol according to [ICAO_SAC]
2. Authentication Mechanism based on AES[42]
3. none[43]

**Application Note 11**: For the PACE protocol, the TOE randomly selects a nonce *s* of 128 bits length being (almost) uniformly distributed .

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

[42] [selection: *Triple-DES, AES or other approved algorithms*]

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

**FIA_UAU.5/PACE Multiple authentication**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.5.1/PACE** The TSF shall provide

1. PACE Protocol according to [ICAO_SAC],
2. Passive Authentication according to [TR-03110_3],
3. Secure messaging MAC-ENC mode according to [ICAO_SAC],
4. Symmetric Authentication Mechanism based on AES[44]
5. none[45]

to support user authentication.

**FIA_UAU.5.2/PACE** 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 code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalisation Agent by the Authentication Mechanism with Personalisation Agent Keys[46].
3. none.[47]

**Application Note 12**: Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of ePassport application.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.6.1/PACE** The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful

[44] [selection: *Triple-DES, AES or other approved algorithms*]

[45] [assignment: *list of multiple authentication mechanism(s)*]

[46] [selection: *the Authentication Mechanism with Personalization Agent Keys*]

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

run of the PACE protocol shall be verified as being sent by the PACE terminal. [48]

**Application Note 13:** The PACE protocol specified in [ICAO_SAC] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

### 7.1.2.3 Class FDP User Data Protection

**FDP_ACC.1/TRM Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM

**FDP_ACC.1.1/TRM** The TSF shall enforce the Access Control SFP[49] on terminals gaining access to the User Data stored in the travel document and data in EF.SOD of the logical travel document[50].

**FDP_ACF.1/TRM Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

**FDP_ACF.1.1/TRM** The TSF shall enforce the Access Control SFP[51] to objects based on the following:

1. Subjects:
   a. Terminal
   b. BIS-PACE;

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

[49] [assignment: *access control SFP*]

[50] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[51] [assignment: *access control SFP*]

2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
3. Security attributes:
   a. Authentication status of terminals[52]
4. none[53].

**FDP_ACF.1.2/TRM** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [ICAO_SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE.[54]

**FDP_ACF.1.3/TRM** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[55].

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. none.[56]

**Application Note 14**: The assignment in FDP_ACF.1.1/TRM may be used in order to extend the subjects and objects and corresponding security attributes for documents with more types of security levels as e.g. some data groups additionally secured by Extended Access Control. The assignment in FDP_ACF.1.4/TRM may be used in order to deny access to DG3 and DG4 as it is recommended [ICAO_9303_1] or to further regulate the access to the objects of FDP_ACF.1.1/TRM. This can be done by the ST writer or in a PP claiming conformance to PACE PP.

---

[52] [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*]

[53] [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*]

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

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

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

**Application Note 15**: Please note that the Document Security Object ($SO_D$) stored in EF.SOD (see [TR-03110_3]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by the PACE authenticated BIS-PACE, see [TR-03110_3]).

**Application Note 16**: Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

### FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

**FDP_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[57] the following objects:

1. Session Keys (immediately after closing related communication session),
2. the ephemeral private key ephem $SK_{PICC}$ PACE (by having generated a DH shared secret K[58]),
3. none[59].

### FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to: No other components.

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

**FDP_UCT.1.1/TRM** The TSF shall enforce the Access Control SFP[60] to be able to transmit and receive[61] user data in a manner protected from unauthorised disclosure.

[57] [selection: *allocation of the resource to, deallocation of the resource from*]

[58] according to [TR-03110_3], sec. 4.2.1, #3.b

[59] [assignment: *list of objects*]

[60] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[61] [selection: *transmit, receive*]

**FDP_UIT.1/TRM Data exchange integrity**

Hierarchical to: No other components.

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

**FDP_UIT.1.1/TRM** The TSF shall enforce the Access Control SFP[62] to be able to transmit and receive[63] user data in a manner protected from modification, deletion, insertion and replay[64] errors.

**FDP_UIT.1.2/TRM** The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[65] has occurred.

### 7.1.2.4 Class FTP Trusted Path/Channels

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

**FTP_ITC.1.3/PACE** The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal. [66]

**Application Note 17:** The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word ´initiate´ is changed to 'enforce´, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

**Application Note 18:** The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was

[62] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[63] [selection: *transmit, receive*]

[64] [selection: *modification, deletion, insertion, replay*]

[65] [selection: *modification, deletion, insertion, replay*]

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

successfully performed, secure messaging is immediately started using the derived session keys: this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.
The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

**Application Note 19**: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

#### 7.1.2.5 Class FAU Security Audit

### FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

**FAU_SAS.1.1** The TSF shall provide the Manufacturer[67] with the capability to store the Initialisation and Pre-Personalisation Data [68] in the audit records.

**Application Note 20:** The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

#### 7.1.2.6 Class FMT Security Management

### FMT_SMF.1 Specification of Management

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Initialization,
2. Pre-personalisation,
3. Personalisation
4. Configuration.[69]

[67] [assignment: *authorised users*]

[68] [assignment: *list of audit information*]

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

**FMT_SMR.1/PACE Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by Application **Note 8**: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [ICAO_SAC]) or for an arbitrary subset of them or may also separately be defined for each datum in question.Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy52, the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack53 requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current PP.One of some opportunities for performing this operation might be '*consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'*.
FIA_UID.1/PACE

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

1. Manufacturer,
2. Personalisation Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. none[70].

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

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

**FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

**FMT_MTD.1.1/INI_DIS** The TSF shall restrict the ability to read out[71] the Initialisation Data and the Pre-personalisation Data [72] to the Personalisation Agent. [73]

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

**Application Note 21:** The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

**FMT_MTD.1.1/KEY_READ** The TSF shall restrict the ability to read[74] the

1. PACE passwords,
2. Personalization Agent Keys
3. **none**[75]

to none[76].

**Application Note 22 (of the ST author):** A refinement has been added to this SFR to also cover the private key for the Active Authentication mechanism.

### FMT_MTD.1/PA Management of TSF data – Personalisation Agent

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

**FMT_MTD.1.1/PA** The TSF shall restrict the ability to write [77] the Document Security Object ($SO_D$)[78] to the Personalisation Agent. [79]

---

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

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

[73] [assignment: *the authorised identified roles*]

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

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

[76] [assignment: *the authorised identified roles*]

**Application Note 23:** By writing $SO_D$ into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

#### 7.1.2.7 Class FPT Protection of the Security Functions

**FPT_EMS.1 TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_EMS.1.1** The TOE shall not emit information about IC power consumption and command execution time[80] in excess of non useful information[81] enabling access to

1. PACE Session Keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$)
2. the ephemeral private key ephem $SK_{PICC}$-PACE
3. Personalisation Agent Key(s)
4. none[82].

**FPT_EMS.1.2** The TSF shall ensure any users[83] are unable to use the following interface smart card circuit contacts[84] to gain access to

1. PACE Session Keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$)
2. the ephemeral private key ephem $SK_{PICC}$-PACE
3. Personalisation Agent Key(s)
4. none[85].

**Application Note 24:** The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to

---

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

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

[79] [assignment: *the authorised identified roles*]

[80] [assignment: *types of emissions*]

[81] [assignment: *specified limits*]

[82] [assignment: *list of types of user data*]

[83] [assignment: *type of users*]

[84] [assignment: *type of connection*]

[85] [assignment: *list of types of user data*]

implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [14] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

**FPT_FLS.1 Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1,
3. none[86]

### 7.1.3 SFRs specifically from [PP_BAC]

For the dependencies of the SFRs specifically from [PP_BAC] please refer to [PP_BAC] section 6.3.2 "Dependency Rationale"

#### 7.1.3.1 FCS: Cryptographic Support

**FCS_CKM.1 Cryptographic key generation – Generation of Document Basic Access Keys by the TOE**

Hierarchical to: No other components.

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

**FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[87] and specified cryptographic key sizes 112 bits[88] that meet the following: [TR-03110_1], normative appendix 5[89].

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

[87] [assignment: *cryptographic key generation algorithm*]

[88] [assignment: *cryptographic key sizes*]

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

**Application Note 25:** The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [TR-03110_1], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [TR-03110_1], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

**FCS_COP.1/SHA Cryptographic operation – Hash for key derivation**

Hierarchical to: No other components.

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

**FCS_COP.1.1/SHA** The TSF shall perform hashing[90] in accordance with a specified cryptographic algorithm SHA-1[91,92] and cryptographic key sizes none[93] that meet the following: FIPS 180-2[94,95].

**Application Note 26:** This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive to derive the Basic Access Control Authentication Mechanism (see also FAU_UAU.4) according to [TR-03110_1].

**FCS_COP.1/ENC Cryptographic operation – Symmetric Encryption / Decryption Triple DES**

Hierarchical to: No other components.

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

**FCS_COP.1.1/ENC** The TSF shall perform secure messaging (BAC) – encryption and decryption[96] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[97] and cryptographic key sizes 112 bits[98] that

[90] [assignment: *list of cryptographic operations*]

[91] [selection: *SHA-1 or other approved algorithms*]

[92] [assignment: *cryptographic algorithm*]

[93] [assignment: *cryptographic key sizes*]

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

[95] [selection: *FIPS 180-2 or other approved standards*]

[96] [assignment: *list of cryptographic operations*]

[97] [assignment: *cryptographic algorithm*]

[98] [assignment: *cryptographic key sizes*]

meet the following: FIPS 46-3 [ISO15946-2] and [TR-03110_1]; normative appendix 5, A5.3[99].

**Application Note 27:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

**FCS_COP.1/AUTH Cryptographic operation – Authentication**

Hierarchical to: No other components.

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

**FCS_COP.1.1/AUTH** The TSF shall perform symmetric authentication – encryption and decryption[100] in accordance with a specified cryptographic algorithm AES[101,102] and cryptographic key sizes 128 bits[103,104] that meet the following: FIPS197 [ISO15946-1][105,106].

**Application Note 28:** This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

**FCS_COP.1/MAC Cryptographic operation – Retail MAC**

Hierarchical to: No other components.

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

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

[100] [assignment: *list of cryptographic operations*]

[101] [selection: *Triple-DES, AES*]

[102] [assignment: *cryptographic algorithm*]

[103] [selection: *112, 128, 168, 192, 256*]

[104] [assignment: *cryptographic key sizes*]

[105] [selection: *FIPS 46-3* [ISO15946-1]], *FIPS 197 [12]*]

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

**FCS_COP.1.1/MAC** The TSF shall perform secure messaging – message authentication code[107] in accordance with a specified cryptographic algorithm Retail-MAC[108] and cryptographic key sizes 112 bits[109] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[110].

**Application Note 29:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

### 7.1.3.2 Class FIA Identification and Authentication

**FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

1. to read the Initialization Data in Phase 2 “Manufacturing”,
2. to read random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[111]

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

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

**Application Note 30:** The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the

[107] [assignment: *list of cryptographic operations*]

[108] [assignment: *cryptographic algorithm*]

[109] [assignment: *cryptographic key sizes*]

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

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

TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

**Application Note 31:** In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier is fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.

The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (Common Criteria Part 2).

**FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

**FIA_UAU.1.1** The TSF shall allow

1. To read the Initialization Data in Phase 2 “Manufacturing”,
2. to read the random identifier in Phase 3 “Personalization of the MRTD”,
3. to read the random identifier in Phase 4 “Operational Use”[112]

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

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

**Application Note 32:** The Basic Inspection System and the Personalization Agent authenticate themselves.

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Basic Access Control Authentication Mechanism,

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

2. Authentication Mechanism based on AES[113,114].

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

**FIA_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.5.1** The TSF shall provide

1. Basic Access Control Authentication Mechanism,
2. Symmetric Authentication Mechanism based on *AES*[115,116]

to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s) Symmetric Authentication Mechanism with Personalization Agent Key[117].
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of Basic Access Control Authentication Mechanism with the Document Basic Access Keys[118].

The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.6.1** The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication

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

[114] [selection: *Triple-DES, AES or other approved algorithms*]

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

[116] [selection: *Triple-DES, AES*]

[117] [selection: *the Basic Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]*]

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

after successful authentication of the terminal with Basic Access Control Authentication Mechanism[119].

**Application Note 33:** The Basic Access Control Mechanism specified in [TR-03110_1] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

**Application Note 34:** Note that in case the TOE should also fulfil [PP_EAC] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

The TOE shall meet the requirement “Authentication failure handling (FIA_AFL.1)” as specified below (Common Criteria Part 2).

**FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

**FIA_AFL.1.1** The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 15 consecutive[120] unsuccessful authentication attempts occur related to the BAC mechanism[121].

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met[122], the TSF shall mute the TOE at the 16th unsuccessful authentication attempt [123].

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

[120] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[121] [assignment: *list of authentication events*]

[122] [assignment: *met or surpassed*]

[123] [assignment: *list of actions*]

**Application Note 35:** These assignments are assigned to ensure especially the strength of authentication function as terminal part of the Basic Access Control Authentication Protocol to resist enhanced basic attack potential.

The terminal challenge $e_{IFD}$ and the TSF response $e_{ICC}$ are described in [ICAO_9303_11], Appendix C. The refinement by inclusion of the word "consecutive" allows the TSF to return to normal operation of the BAC authentication protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the "consecutive unsuccessful authentication attempts" are count independent on power-on sessions but reset to zero after successful authentication only.

### 7.1.3.3 Class FDP User Data Protection

**Subset access control (FDP_ACC.1)**

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

**FDP_ACC.1 Subset access control – Basic Access Control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

**FDP_ACC.1.1** The TSF shall enforce the Basic Access Control SFP[124] on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[125].

**Security attribute based access control (FDP_ACF.1)**

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

**FDP_ACF.1.1** The TSF shall enforce the Basic Access Control SFP[126] to objects based on the following:

[124] [assignment: *access control SFP*]

[125] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[126] [assignment: *access control SFP*]

i. Subjects:
   1. Personalization Agent,
   2. Basic Inspection System,
   3. Terminal,

ii. Objects:
   1. data EF.DG1 to EF.DG16 of the logical MRTD,
   2. data in EF.COM,
   3. data in EF.SOD

iii. Security attributes:
   1. authentication status of terminals[127]

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

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD[128]

**FDP_ACF.1.3** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[129].

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

1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.[130]

**Application Note 36:** The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this protection profile (cf. [PP_EAC] for details).

**Inter-TSF-Transfer**

[127] [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*]

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

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

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

**Application Note 37:** FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

**FDP_UCT.1 Basic data exchange confidentiality - MRTD**

Hierarchical to: No other components.

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

**FDP_UCT.1.1** The TSF shall enforce the Basic Access Control SFP[131] to be able to transmit and receive[132] user data in a manner protected from unauthorized disclosure.

**FDP_UIT.1 Data exchange integrity - MRTD**

Hierarchical to: No other components.

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

**FDP_UIT.1.1** The TSF shall enforce the Basic Access Control SFP[133] to be able to transmit and receive[134] user data in a manner protected from modification, deletion, insertion and replay[135] errors.

**FDP_UIT.1.2** The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[136] has occurred.

### 7.1.3.4 Class FAU Security Audit

**FAU_SAS.1/BAC Audit storage**

[131] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[132] [selection: *transmit, receive*]

[133] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[134] [selection: *transmit, receive*]

[135] [selection: *modification, deletion, insertion, replay*]

[136] [selection: *modification, deletion, insertion, replay*]

Hierarchical to: No other components.

Dependencies: No dependencies.

**FAU_SAS.1.1/BAC** The TSF shall provide the Manufacturer[137] with the capability to store the IC Identification Data[138] in the audit records.

**Application Note 38:** The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1.1/INI_DIS).

### 7.1.3.5 Class FMT Security Management

#### FMT_SMF.1/BAC Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Initialization,
2. Pre-Personalization,
3. Personalization[139]

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

#### FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

**FMT_SMR.1.1** The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Basic Inspection System.[140]

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

---

[137] [assignment: *authorised users*]

[138] [assignment: *list of audit information*]

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

[140] [assignment: *the authorised identified roles*]

**Application Note 39:** The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 extended).

**FMT_LIM.1/BAC Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1/BAC 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 disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[141]

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (Common Criteria Part 2 extended).

**FMT_LIM.2/BAC Limited availability**

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

**FMT_LIM.2.1/BAC** 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,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.[142]

**Application Note 40:** The formulation of “Deploying Test Features …” in **FMT_LIM.2.1** might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality).

[141] [assignment: *limited capability and availability policy*]

[142] [assignment: *limited capability and availability policy*]

Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1 and **FMT_LIM.2.1** refers to both IC Dedicated and IC Embedded Software.

**Application Note 41:** The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/INI_DIS/BAC** The TSF shall restrict the ability to disable read access for users to[143] the Initialization Data[144] to the Personalization Agent[145].

**Application Note 42:** The IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE restricts the ability to write the Initialization Data and the Pre-personalization Data by blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “Personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/KEY_WRITE** The TSF shall restrict the ability to write[146] the Document Basic Access Keys[147] to the Personalization Agent[148].

---

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

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

[145] [assignment: *the authorised identified roles*]

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

**FMT_MTD.1/KEY_READ_BAC Management of TSF data –Key Read**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/KEY_READ/BAC** The TSF shall restrict the ability to read[149] the Document Basic Access Keys and Personalization Agent Keys[150] to none[151].

**Application Note 43:** The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

### 7.1.3.6 Class FPT Protection of the Security Functions

**FPT_EMSEC.1 TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_EMSEC.1.1** The TOE shall not emit information about IC power consumption and command execution time[152] in excess of non useful information[153] enabling access to Personalization Agent Key(s)[154] and logical MRTD data[155].

**FPT_EMSEC.1.2** The TSF shall ensure any unauthorized users[156] are unable to use the following interface smart card circuit contacts[157] to gain access to Personalization Agent Key(s)[158] and logical MRTD data[159].

**Application Note 44:** The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE.

---

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

[148] [assignment: *the authorised identified roles*]

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

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

[151] [assignment: *the authorised identified roles*]

[152] [assignment: *types of emissions*]

[153] [assignment: *specified limits*]

[154] [assignment: *type of users*]

[155] [assignment: *list of types of user data*]

[156] [assignment: *type of users*]

[157] [assignment: *type of connection*]

[158] [assignment: *type of users*]

[159] [assignment: *list of types of user data*]

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

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

**FPT_FLS.1/BAC Failure with preservation of secure state**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1[160]

## 7.1.4 SFRs specifically from [PP_EAC] and for the Active Authentication (AA)

### 7.1.4.1 Cryptographic support

**FCS_CKM.1/CA Cryptographic key generation**

Hierarchical to: No other components.

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

**FCS_CKM.1.1/CA** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to ISO

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

15946[161,162] and specified cryptographic key sizes 112 bits[163], 128, 192, 256 bits[164], 192 bits – 521 bits[165,166] that meet the following: TR03111 [TR-3111][167].

**Application Note 45:** The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [TR-03110_1], sec. 3.1 and Annex A.1. This protocol is based on the ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [TR-03110_1], Annex A.1, [TR-3111] and [ISO15946-3] for details). The shared secret value is used to derive Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [TR-03110_1], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/ and FCS_COP.1.1/MAC.

#### 7.1.4.2 Cryptographic operations

**FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption**

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

**FCS_COP.1.1/CA_ENC** The TSF shall perform secure messaging – encryption and decryption[168] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode, AES[169] and cryptographic key sizes 112 bits, 128 bits[170] that meet the following: FIPS PUB 46-3 [ANSIX962], FIPS PUB 197 [SP800-20] Chapter 5[171].

---

[161] [selection: *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946*]

[162] [assignment: *cryptographic key generation algorithm*]

[163] Bit length of 2-key Triple DES session keys

[164] Bit length of AES session keys

[165] Bit length of the curve

[166] [assignment: *cryptographic key sizes*]

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

[168] [assignment: *list of cryptographic operations*]

[169] [assignment: *cryptographic algorithm*]

[170] [assignment: *cryptographic key sizes*]

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

**Application Note 46:** This SFR requires the TOE to implement the cryptographic primitives (Triple-DES and AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

**FCS_COP.1/SIG_VER Cryptographic operation – Signature verification**

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

**FCS_COP.1.1/SIG_VER** The TSF shall perform digital signature verification[172] in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[173] and cryptographic key sizes 192-521 bits[174,175] that meet the following: ISO/IEC 14888-3 [ISO/IEC 14888-3], Chapter 6.4[176].

**Application Note 47:** The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

**Application Note 48:** The TOE uses the following ECC brainpool curves: P224r1, P256r1, P320r1, see chapter 1.3.2 [TR-3116-2] and NIST curves: P-256 (secp256r1), P-384 (secp384r1) and P-521 (secp521r1), see [TR-03110_3].

**Application Note 49:** Padding is applied as described in Section 6.4.3.5 of ISO/IEC 14888-3 ISO/IEC 14888-3]. For example in case of SHA-512 hash function and P-521 curve, the hash-code H = h(M) of message M is converted to an integer according to the conversion rule BS2I given in Annex B of ISO14888-3.

**FCS_COP.1/SIG_GEN Cryptographic operation – Signature generation**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: This SFR is not used to calculate any shared secrets, nor does it import user data. Therefore there is no need for security attributes.
FCS_CKM.4 Cryptographic key destruction: Fulfilled by FCS_CKM.4

[172] [assignment: *list of cryptographic operations*]

[173] [assignment: *cryptographic algorithm*]

[174] [assignment: *cryptographic key sizes*]

[175] Bit length of curve

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

**FCS_COP.1.1/SIG_GEN** The TSF shall perform signature generation[177] in accordance with a specified cryptographic algorithm RSA[178] and cryptographic key sizes 1024, 1280, 1536, 1984, 2048 bit or ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[179] and cryptographic key sizes 192-521 bits[180] that meet the following scheme 1 of [ISO9796-2] chapter 8 and [PKCS1] chapter 8.2 (RSASSA-PKCS1-v1_5) for RSA signatures and [TR-03110_1] for ECDSA signatures[181].

### FCS_COP.1/CA_MAC Cryptographic operation – MAC

Hierarchical to: No other components.

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

**FCS_COP.1.1/CA_MAC** The TSF shall perform secure messaging – message authentication code[182] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode, AES[183] and cryptographic key sizes 112 bits, 128 bits[184] that meet the following: FIPS PUB 46-3 [ANSIX962], FIPS PUB 197 [SP800-20] Chapter 5[185].

**Application note 50:** The TOE implements the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

#### 7.1.4.3 Class FIA Identification and Authentication

**Application Note 29:** The Table 7 provides an overview of the authentication mechanisms used.

---

[177] [assignment: *list of cryptographic operations*]

[178] [assignment: *cryptographic algorithm*]

[179] [assignment: *cryptographic algorithm*]

[180] [assignment: *cryptographic key sizes*]

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

[182] [assignment: *list of cryptographic operations*]

[183] [assignment: *cryptographic algorithm*]

[184] [assignment: *cryptographic key sizes*]

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

| Name | SFR for the TOE |
|---|---|
| Symmetric Authentication Mechanism for Personalization Agents | FIA_UAU.4 |
| Chip Authentication Protocol | FIA_AFL.1, FIA_UAU.5, FIA_UAU.6 |
| Terminal Authentication Protocol | FIA_UAU.5 |
| Active Authentication Mechanism | FIA_API.1/AA |

**Table 7 Overview on authentication SFRs**

Note the Chip Authentication Protocol as defined in this security target[186] includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [TR-03110_1]in order to gain access to the Chip Authentication Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

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

### FIA_UID.1/PACE_EAC Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UID.1.1/PACE_EAC** The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO_SAC],
3. to read the Initialisation Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol Version 1 according to [TR-03110_1]
5. to carry out the Terminal Authentication Protocol Version 1 according to [TR-03110_1]
6. none[187]

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

[186] The BAC Authentication Protocol is included here as part of the Chip Authentication Protocol because it is a necessary condition to read the EF.DG14.

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

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

**Application Note 51:** In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the Document Basic Access Keys, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Basic Inspection System (cf. PP MRTD BAC [PP_BAC]) is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to run the BAC Authentication Protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol (i.e. the BAC mechanism is not seen as an independent mechanism in this ST, it is a mandatory part within the Chip Authentication Protocol, and thus noted here for reasons of completeness). After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol or (ii) if necessary and available by symmetric authentication as Personalization Agent (using the Personalization Agent Key).

### FIA_UAU.1/PACE_EAC Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

**FIA_UAU.1.1/PACE_EAC** The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO_SAC],
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key,
5. to carry out the Chip Authentication Protocol Version 1 according to [TR-03110_1]
6. to carry out the Terminal Authentication Protocol Version 1 according to [TR-03110_1]
7. none[188]

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

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

### FIA_UAU.4/PACE_EAC Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

1. PACE Protocol according to [ICAO_SAC],
2. Authentication Mechanism based on AES,[189]
3. Terminal Authentication Protocol v.1 according to [TR-03110_1][190]

**Application Note 52**: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

### FIA_UAU.5/PACE_EAC Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.5.1/PACE_EAC** The TSF shall provide

1. PACE Protocol according to [ICAO_SAC],
2. Passive Authentication according to [TR-03110_3],
3. Secure messaging in MAC-ENC mode according to [ICAO_SAC],
4. Symmetric Authentication Mechanism based on AES[191,192]
5. Terminal Authentication Protocol v.1 according to [TR-03110_1],

to support user authentication.

**FIA_UAU.5.2/PACE_EAC** 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 code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key[193].

---

[189] [selection: *Triple-DES, AES or other approved algorithms*]

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

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

[192] [selection: *Triple-DES, AES or other approved algorithms*]

[193] [selection: *the Symmetric Authentication Mechanism with Personalization Agent Key, the Terminal Authentication Protocol with Personalization Agent Keys*]

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 v.1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism v.1.[194]
5. none[195].

**Application Note 53:** Depending on the authentication methods used the Personalization Agent holds (i) a key for the Symmetric Authentication Mechanism or (ii) an asymmetric key pair for the Terminal Authentication Protocol (e.g. provided by the Extended Access Control PKI in a valid card verifiable certificate with appropriate encoded access rights). The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys and the secure messaging after the mutual authentication. The General Inspection System shall use the secure messaging with the keys generated by the Chip Authentication Mechanism.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_UAU.6.1/EAC** The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System[196].

**Application Note 54:** The Basic Access Control Mechanism and the Chip Authentication Protocol specified in [TR-03110_1] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE reauthenticates the user for each received command and accepts only those commands received from the previously authenticated user.

### FIA_API.1 Authentication Proof of Identity

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

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

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

Hierarchical to: No other components.

Dependencies:No dependencies.

**FIA_API.1.1** The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR-03110_1][197] to prove the identity of the TOE[198].

**Application note 55:** This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR-03110_1]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO_9303_1]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

**FIA_API.1/AA Authentication Proof of Identity – MRTD**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA_API.1.1/AA** The TSF shall provide the Active Authentication Mechanism according to [TR-03110_1][199] to prove the identity of the TOE[200].

### 7.1.4.4 Class FDP User Data Protection

**FDP_ACC.1/TRM_EAC Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

**FDP_ACC.1.1/TRM_EAC** The TSF shall enforce the Access Control SFP[201] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document[202].

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

[197] [assignment: *authentication mechanism*]

[198] [assignment: *authorized user or role*]

[199] [assignment: *authentication mechanism*]

[200] [assignment: *authorized user or role*]

[201] [assignment: *access control SFP*]

[202] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

**FDP_ACF.1/TRM_EAC Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

**FDP_ACF.1.1/TRM_EAC** The TSF shall enforce the Access Control SFP[203] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. BIS-PACE,
   c. Extended Inspection System
2. Objects:
   a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document,
   b. data EF.DG3 and EF.DG4 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document[204]
3. Security attributes:
   a. PACE Authentication
   b. Terminal Authentication v.1
   c. Authorisation of the Terminal[205]

**FDP_ACF.1.2/TRM_EAC** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [ICAO_SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE[206].

**FDP_ACF.1.3/TRM_EAC** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[207].

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

---

[203] [assignment: *access control SFP*]

[204] e.g. Chip Authentication Version 1 and ephemeral keys

[205] [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*]

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

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM,
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4[208].

**Application Note 56:** The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR-03110_1], Annex A.5.1, table A.8. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

**Application Note 57:** Please note that the Document Security Object ($SO_D$) stored in EF.SOD (see [ICAO_9303_1]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [ICAO_SAC].

**Application note 58:** FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

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

### 7.1.4.5 Class FMT Security Management

**FMT_SMR.1/PACE_EAC Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

**FMT_SMR.1.1/PACE_EAC** The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System,
8. Foreign Extended Inspection System.[209]

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

**Application note 59:** Note that the MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC_PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

**Application note 60:** The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

**FMT_LIM.1 Limited capabilities**

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability fulfilled by FMT_LIM.2.

**FMT_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed,

[209] [assignment: *the authorised identified roles*]

4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[210].

**FMT_LIM.2 Limited availability**

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities fulfilled by FMT_LIM.2

**FMT_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow:

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[211].

**Application Note 61:** Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

**Application note 62:** The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/CVCA_INI** The TSF shall restrict the ability to write[212] the

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

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

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

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date
4. none[213]

to the Personalization Agent[214].

**Application Note 63:** The initial Country Verifying Certification Authority Public Key is written by the Personalization Agent (cf. [TR-03110_1], sec. 2.2.6). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/CVCA_UPD** The TSF shall restrict the ability to update[215] the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[216]

to Country Verifying Certification Authority[217].

**Application Note 64:** The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [TR-03110_1], sec. 2.2). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [TR-03110_1], sec. 2.2.3 and 2.2.4).

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

---

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

[214] [assignment: *the authorised identified roles*]

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

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

[217] [assignment: *the authorised identified roles*]

**FMT_MTD.1.1/DATE** The TSF shall restrict the ability to modify[218] the Current date[219] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System[220].

**Application Note 65:** The authorized roles are identified in their certificate (cf. [TR-03110_1], sec. 2.2.4 and Table A.5) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. [TR-03110_1], annex A.3.3, for details).

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/CAPK** The TSF shall restrict the ability to create, load[221] the Chip Authentication Private Key[222] to the Manufacturer and the Personalization Agent[223].

**Application note 66:** The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself.

**FMT_MTD.1/KEY_READ_EAC Management of TSF data –Key Read**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/KEY_READ_EAC** The TSF shall restrict the ability to read[224] the

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

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

[220] [assignment: *the authorised identified roles*]

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

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

[223] [assignment: *the authorised identified roles*]

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

1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalization Agent Keys
4. Active Authentication Private Key[225]

to none[226].

**FMT_MTD.3 Secure TSF data**

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

**FMT_MTD.3.1** The TSF shall ensure that only secure **values of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[227].

**Refinement: The certificate chain is valid if and only if**

**(1) the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**

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

**(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.**

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

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

**Application note 50:** The Terminal Authentication is used for Extended Inspection System as required by **FIA_UAU.4** and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

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

[226] [assignment: *the authorised identified roles*]

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

**FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key**

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

**FMT_MTD.1.1/AAPK** The TSF shall restrict the ability to create, load[228] the Active Authentication Private Key[229] to the Manufacturer and the Personalization Agent[230].

### 7.1.4.6 Class FPT Protection of the Security Functions

**FPT_EMS.1/EAC TOE Emanation**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_EMS.1.1/EAC** The TOE shall not emit information about IC power consumption and command execution time[231] in excess of non useful information[232] enabling access to

1. Chip Authentication Session Keys
2. PACE Session Keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$)
3. the ephemeral private key ephem $SK_{PICC}$-PACE
4. Personalisation Agent Key(s)
5. Chip Authentication Private Key
6. Active Authentication Private Key[233] and
7. none[234].

**FPT_EMS.1.2/EAC** The TSF shall ensure any users[235] are unable to use the following interface smart card circuit contacts[236] to gain access to

1. Chip Authentication Session Keys

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

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

[230] [assignment: *the authorised identified roles*]

[231] [assignment: *types of emissions*]

[232] [assignment: *specified limits*]

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

[234] [assignment: *list of types of user data*]

[235] [assignment: *type of users*]

[236] [assignment: *type of connection*]

2. PACE Session Keys (PACE-$K_{MAC}$, PACE-$K_{ENC}$)
3. the ephemeral private key ephem $SK_{PICC}$-PACE
4. Personalisation Agent Key(s)
5. Chip Authentication Private Key
6. Active Authentication Private Key[237] and
7. none[238].

**Application Note 67:** The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [14] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

## 7.2 Security Assurance Requirements

For the BAC feature, the TOE claims EAL 4 augmented with ALC_DVS.2 and ATE_DPT.2, therefore [PP_BAC] section 6.2 "Security Assurance Requirements for the TOE" applies.

For PACE and PACE-EAC features, the current document claims EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 therefore it claims a higher assurance level compared to [PP_SAC] and [PP_EAC], section 6.2 respectively.

## 7.3 Security Requirements Rationale

### 7.3.1 Security Functional Requirements Rationale

Respective sections 6.3.1 "Security Functional Requirements Rationale" of [PP_SAC], [PP_BAC] and [PP_EAC] are applicable for this chapter.

For the additionally defined SFRs in this ST, FIA_API.1/AA, FMT_MTD.1/AAPK and FCS_COP.1/SIG_GEN formalizing the Active Authentication feature they meet the security objective OT.Active_Auth together with FMT_MTD.1.1/KEY_READ_EAC, FPT_EMS.1/EAC from [PP_EAC].

[237] [assignment: *type of users*]

[238] [assignment: *list of types of user data*]

### 7.3.2 Rationale for SFR's Dependencies

[PP_SAC], [PP_BAC] and [PP_EAC] section 6.3.2 "Rationale for SFR's Dependencies" are also applicable for this chapter.

### 7.3.3 Security Assurance Requirements Rationale

[PP_BAC] section 6.3.3 "Security Assurance Requirements Rationale " is applicable for this chapter. Additionally due to the old CC version on which PP0055 is based ATE_DPT.2 is added.

[PP_EAC] and [PP_SAC] and their respective sections 6.3.3 "Security Assurance Requirements Rationale" are also applicable for this chapter with one additional rationale justifying the security assurance dependencies.

With the exception of ALC_DVS.2 and AVA_VAN.5, all assurance components are part of the EAL5 package, which by package design does not have any dependency conflicts and is hierarchical to EAL4. The assurance components ALC_DVS.2 and AVA_VAN.5 are also part of the assurance requirements from [PP_SAC], where assurance dependencies are met as is shown in section 6.3.3 from [PP_SAC].

EAL5+ augmented with ALC_DVS.2 and AVA_VAN.5 is appropriate for this TOE, because this assurance level is requested by several states. The assurance expectations for this kind of application are high due to the sensitivity of data stored by the TOE. Therefore several governmental organizations request for an increased assurance level.

### 7.3.4 7.3.4 Security Requirements – Internal Consistency

The rationale for the internal consistency of the SFRs from [PP_SAC], [PP_BAC] and [PP_EAC] section 6.3.4 "Security Requirements – Internal Consistency" are also applicable to this chapter.

The assurance package EAL5 and EAL4 are pre-defined sets of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in [PP_SAC], [PP_EAC] and [PP_BAC] section 7.3.3 "Security Assurance Requirements Rationale" together with the additional rational from section 7.3.3 show that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

The rationale for internal consistency between functional and assurance requirements from [PP_SAC], [PP_EAC] and and [PP_BAC] section 6.3.4 "Security Requirements – Internal Consistency" are also applicable to this chapter.

# 8 TOE summary specification

## 8.1 TOE Security functions

This chapter gives the overview description of the different TOE Security Functions composing the TSF.

### 8.1.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users (Manufacturer, Personalisation Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), domestic Extended Inspection System, foreign Extended Inspection System).

The TOE restricts the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. Manufacturer is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

Personalisation Agent is the only role with the ability:

- to disable read access for users to the Initialisation Data.
- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date.
- to write the Document Basic Access Keys and the chip authentication private key (which may also be written by the manufacturer).
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document after successful authentication.

No terminal is allowed

- to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
- to read any of the EF.DG1 to EF.DG16 of the logical MRTD.

The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys and the Personalization Agent Keys.

The access control mechanisms ensure that only the Country Verifying Certification Authority has the ability to update the CVCA Public Key and the CVCA Certificate.

The access control mechanisms ensure that only authenticated Extended Inspection System with the Read access to

- DG 3 (Fingerprint) is allowed to read the data in EF.DG3 of the logical travel document.

- DG 4 (Iris) is allowed to read the data in EF.DG4 of the logical travel document.

The successfully with PACE authenticated Basic Inspection System (BIS-PACE) terminal is allowed to read data from EF.DG1, EF.DG2, EF.DG3, EF.DG4 and EF.DG5 to EF.DG16 of the logical travel document, read data of the logical document.

The TOE maintains the role Basic Inspection System.

The successfully authenticated Basic Inspection System is allowed to read data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.

Terminals not using secure messaging are not allowed to read, to modify, to write or to use any data stored on the travel document

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

In all other cases, reading any of the EF.DG3 to EF.DG4 of the logical travel document is explicitly denied.

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

A terminal authenticated as CVCA or as DV is explicitly denied to read data in the EF.DG3 and EF.DG4.

Any terminal is explicitly denied to modify any of the EF.DG1 to EF.DG16 of the logical travel document.

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

Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be manipulated, sensitive User Data (EF.DG3 and EF.DG4) to be disclosed, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks.

The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

The TOE provides management functions for configuration, initialization, pre-personalization and personalization.

The TOE does not allow user data to be disclosed after TOE delivery.

The TOE provides the manufacuterer and the peresonalization agent to create and load the Active Authentication Private key.

The TOE allows the personalization agent to read out the initialisation data and the pre-personalization data.

The TOE provides the CVCA, DV and Domestic Extended Inspection system the ability to modify the current date.

The TOE allows the Personalization agent to write the document security object (SOd).

The TOE allows nobody to read the PACE passwords.

### 8.1.2 SF_Authentication

After activation or reset of the TOE no user is authenticated.

TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

The TOE contains a deterministic random number generator rated DRG.3 according to AIS20 [AIS20] that provides random numbers used authentication. The seed for the deterministic random number generator is provided by the PTG.2 true random number generator [AIS31] of the underlying IC.

The TOE supports user authentication by the following means:

- Basic Access Control Authentication Mechanism (if a BIS chooses BAC as authentication method)
- PACE Protocol (PACE with generic mapping and PACE-CAM)
- Terminal Authentication Protocol
- Secure messaging in MAC-ENC mode
- Symmetric Authentication Mechanism based on AES
- Chip Authentication authenticates the Genreral inspection system

Proving the identity of the TOE is supported by the following means:

- Chip Authentication Protocol
- Active Authentication Mechanism

The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol
- Symmetric Authentication Mechanism based on AES

The Personalisation Agent authenticates himself to the TOE by use of the Personalisation Agent Keys with the following cryptographic mechanism:

- Symmetric Authentication Mechanism based on AES

After completion of the PACE Protocol or the Chip Authentication Protocol, the TOE accepts commands with correct message authentication code only. These commands must have been sent via secure messaging using the key previously agreed with the terminal during the last authentication.

The TOE accepts terminal authentication attempts by means of the Terminal Authentication Protocol only via secure messaging that was established by the preceding Chip Authentication Protocol.

The TOE verifies each command received after successful completion of the Chip Authentication Protocol as having been sent by the terminal.

The TOE enforces the Access Control SFP to transmit and receive user data in a manner protected from unauthorised disclosure and modification, deletion, insertion and replay errors

Protection of user data transmitted from the TOE to the terminal is achieved by means of secure messaging with encryption and message authentication codes. After Chip Authentication or PACE or BAC authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay attacks.

The TOE enforces the Basic Access Control SFP to transmit and receive user data in a manner protected from unauthorised disclosure and modification, deletion, insertion and replay errors.

The TOE detects when 15 unsuccessful authentication attempts occurs related to authentication attempts using the PACE password as shared password and when the defined number of unsuccessful authentication attempts has been met, the TOE delays each following authentication attempt until the next successful authentication attempt by approx. 1-10 seconds, the delay increasing on every unsuccessful authentication attempts.

The TOE detects when an administrator configurable positive integer within range of acceptable values 1 to 15 consecutive unsuccessful authentication attempts occurs related to the BAC mechanism. When the defined number of unsuccessful authentication attempts has been met, the TOE waits for an administrator configurable time (1 to 10 seconds) between receiving the terminal challenge $e_{IFD}$ and sending the TSF response $e_{ICC}$ during the BAC authentication attempts.

The TOE performs hashing with SHA-1 for the BAC key derivation.

The TOE performs digital singature verification in accordance with a specifioed cryptographic algorithm ECDSA with SHA.

The TOE performs symmetric authentication –encryption and decryption in accordance with a specifioed cryptographic algorithm AES.

The TOE allows to read out the initialization data in phase 2 Manufacturing, to read the random identifier in phase 3 Personalization of the MRTD and phase 4 Operational Use.

The TOE allows establishing a communication protocol and to read out initializatoin data if not restricted to the Personalization Agent.

The TOE allows authentication by selection of the authentication key.

The TOE prevents reuse of authentication data related to BAC and PACE.

The TSF provides chip authentication protocol version 1 and active authentication to prove the identity of the TOE.

### 8.1.3 SF_AssetProtection

The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

### 8.1.4 SF_TSFProtection

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

The TOE is resistant to physical tampering on the TSF. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state.

### 8.1.5 SF_KeyManagement

The TOE supports onboard generation of cryptographic keys based on the ECDH compliant [TR-3111] as well as generation of RSA and ECC key pairs.

The TOE generates Document Basic Access Keys using the Document basis access key derviation algorithm.

The TOE supports overwriting the cryptographic keys with zero values as follows:

- the BAC Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol,
- the PACE Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol,
- the Chip Authentication Session Keys after detection of an error in a received command by verification of the MAC,
- any session keys before starting the communication with the terminal in a new power-on-session.

## 8.2 Assurance measures

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 7.

The following table lists the Assurance measures and references the corresponding documents describing the measures.

| Assurance Measures | Description |
|---|---|
| AM_ADV | The representation of the TSF is described in the documentation for functional specification, in the documentation for the formal security policy model,in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation. |
| AM_AGD | The guidance documentation is described in the operational guidance documentation and in the documentation for preparative procedures. |
| AM_ALC | The life cycle support of the TOE during its development and maintenance is described in the life cycle documentation including configuration management, delivery procedures, development security as well as development tools. |
| AM_ATE | The testing of the TOE is described in the test documentation. |
| AM_AVA | The evaluator uses the development and guidance documentation by the developer as a basis for his vulnerability analysis. |

**Table 8: Reference of Assurance Measures**

## 8.3 Association tables of SFRs and TSF

| TOE SFR / Security Function | SF_AccessControl | SF_Authentication | SF_AssetProtection | SF_TSFProtection | SF_KeyManagement |
|---|---|---|---|---|---|
| FAU_SAS.1 | x | | | | |
| FAU_SAS.1/BAC | x | | | | |
| FCS_CKM.1 | | | | | x |
| FCS_CKM.1/CA | | | | | x |
| FCS_CKM.1/DH_PACE | | | | | x |
| FCS_CKM.4 | | | | | x |
| FCS_COP.1/CA_ENC | | x | | | |

| TOE SFR / Security Function | SF_AccessControl | SF_Authentication | SF_AssetProtection | SF_TSFProtection | SF_KeyManagement |
|---|---|---|---|---|---|
| FCS_COP.1/CA_MAC | | x | | | |
| FCS_COP.1/PACE_ENC | | x | | | |
| FCS_COP.1/PACE_MAC | | x | | | |
| FCS_COP.1/SHA | | x | | | |
| FCS_COP.1/MAC | | x | | | |
| FCS_COP.1/SIG_VER | | x | | | |
| FCS_COP.1/SIG_GEN | | | | | |
| FCS_COP.1/ENC | | x | | | |
| FCS_COP.1/AUTH | | x | | | |
| FCS_RND.1 | | x | | | |
| FDP_ACC.1/TRM | x | | | | |
| FDP_ACC.1/TRM_EAC | x | | | | |
| FDP_ACF.1 | x | | | | |
| FDP_ACF.1/TRM | x | | | | |
| FDP_ACF.1/TRM_EAC | x | | | | |
| FDP_RIP.1 | | | | | **x** |
| FDP_UCT.1/TRM | | x | | | |
| FDP_UIT.1/TRM | | x | | | |
| FIA_AFL.1 | | x | | | |
| FIA_AFL.1/PACE | | x | | | |
| FIA_UID.1 | | x | | | |
| FIA_UID.1/PACE | | x | | | |
| FIA_UID.1/PACE_EAC | | x | | | |
| FIA_UAU.1 | | x | | | |
| FIA_UAU.1/PACE | | x | | | |
| FIA_UAU.1/PACE_EAC | | x | | | |
| FIA_UAU.4 | | x | | | |
| FIA_UAU.4/PACE | | x | | | |
| FIA_UAU.4/PACE_EAC | | x | | | |

| TOE SFR / Security Function | SF_AccessControl | SF_Authentication | SF_AssetProtection | SF_TSFProtection | SF_KeyManagement |
|---|---|---|---|---|---|
| FIA_UAU.5 | | x | | | |
| FIA_UAU.5/PACE | | x | | | |
| FIA_UAU.5/PACE_EAC | | x | | | |
| FIA_UAU.6 | | x | | | |
| FIA_UAU.6/PACE | | x | | | |
| FIA_UAU.6/EAC | | x | | | |
| FIA_API.1 | | x | | | |
| FIA_API.1/AA | | x | | | |
| FDP_ACC.1 | x | | | | |
| FDP_UCT.1 | | x | | | |
| FDP_UIT.1 | | x | | | |
| FMT_SMF.1 | x | | | | |
| FMT_SMF.1/BAC | x | | | | |
| FMT_SMR.1 | x | | | | |
| FMT_SMR.1/PACE | x | | | | |
| FMT_SMR.1/PACE_EAC | x | | | | |
| FMT_LIM.1 | x | | | | |
| FMT_LIM.1/BAC | x | | | | |
| FMT_LIM.2 | x | | | | |
| FMT_LIM.2/BAC | x | | | | |
| FMT_MTD.1/AAPK | x | | | | |
| FMT_MTD.1/INI_ENA | x | | | | |
| FMT_MTD.1/INI_DIS | x | | | | |
| FMT_MTD.1/INI_DIS/BAC | x | | | | |
| FMT_MTD.1/CVCA_INI | x | | | | |
| FMT_MTD.1/CVCA_UPD | x | | | | |
| FMT_MTD.1/DATE | x | | | | |
| FMT_MTD.1/KEY_WRITE | x | | | | |
| FMT_MTD.1/CAPK | x | | | | |

| TOE SFR / Security Function | SF_AccessControl | SF_Authentication | SF_AssetProtection | SF_TSFProtection | SF_KeyManagement |
|---|---|---|---|---|---|
| FMT_MTD.1/KEY_READ | x | | | | |
| FMT_MTD.1/KEY_READ_BAC | x | | | | |
| FMT_MTD.1/KEY_READ_EAC | x | | | | |
| FMT_MTD.1/PA | x | | | | |
| FMT_MTD.3 | x | | | | |
| FPT_EMS.1 | | | x | | |
| FPT_EMS.1/EAC | | | x | | |
| FPT_EMSEC.1 | | | x | | |
| FPT_TST.1 | | | | x | |
| FPT_FLS.1 | | | | x | |
| FPT_FLS.1/BAC | | | | x | |
| FPT_PHP.3 | | | | x | |
| FTP_ITC.1/PACE | | x | | | |

**Table 9: SFRs and TSF - Coverage**

# 9 References, and Abbreviations

## 9.1 References

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20, Version 3, 15.05.2013, Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren, Zertifizierungsstelle des BSI.

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Funktionalitätsklassen und Evaluierungsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013

[ANSIX962] ANSI X9.62:2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 5, April 2017. CCMB-2017-04-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 5, April 2017. CCMB-2017-04-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components. Version 3.1, Revision 5, April 2017. CCMB-2017-04-003.

[ICAO_9303_1] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Seventh Edition, 2015, International Civil Aviation Organization

[ICAO_9303_10] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

[ICAO_9303_11] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Seventh Edition – 2015 Part 11: Security Mechanisms for MRTD's

[ICAO_SAC] International Civil Aviation Organization Machine Readable Travel DocumentsTechnical Report Supplemental Access Control for Machine Readable Travel Documents Version 1.00, November 2010

[IFX_Cert] Certification report BSI-DSZ-CC-1107-V3-2022 IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance from Infineon Technologies AG

[IFX_ST] Security Target Lite BSI-DSZ-CC-1107-V3--2022, Security Target Lite for the IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, Revision: v4.3.1, 2022-05-10, Infineon

[ISO9796-2] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, Dezember 2010

[ISO9797-1] ISO/IEC 9797-1:2011: Information technology – Security techniques –Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[ISO11770-3] ISO/IEC 11770-3:2015: Information technology – Security techniques – Key management- Part 3: Mechanisms using asymmetric techniques

[ISO/IEC 14888-3] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[ISO15946-1] ISO/IEC 15946-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[ISO15946-2] ISO/IEC 15946-2: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[ISO15946-3] ISO/IEC 15946-3: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[ISO18031] ISO/IEC 18031:2011: Information technology – Security techniques – Random bit generation

[JCAPI31] Java Card Platform, versions 3.1, Classic Edition, Application Programming Interface, November 2019. Published by Sun Microsystems, Inc.

[JCAPI304] Java Card API, Classic Edition. Version 3.0.4., 2011 (Oracle)

[JCRE301] Java Card 3 Platform Runtime Environment Specification, Classic Edition. Version 3.1., November 2019 (Oracle)

[JCSPP] Java Card System - Open Configuration Protection Profile Version 3.1, April 2020, developed by Oracle Corporation, BSI-CC-PP-0099-V2-2020

[JCVM31] Java Card 3 Platform Virtual Machine Specification, Classic Edition. Version 3.1., November 2019 (Oracle)

[PKCS1] PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note, Version 2.2, November, 2016

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

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

[PP_SAC] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, Version 1.0.1, 22th July 2014

[RFC5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, BSI and secunet, March 2010, ISSN 2070-1721

[SCE 8.0 Cert] Certification report Sm@rtCafé® Expert 8.0 C2, NSCIB-CC-23-2300005-01-CR

[SCE 8.0 ST] Security Target Sm@rtCafé® Expert 8.0 C2, Veridos, Version 4.2, 03.08.2023

[SP800-20] NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999

[TR-03110_1] Federal Office for Information Security (BSI) Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 1 - eMRTDs with BAC/PACEv2 and EACv1 Version 2.20, 26. February 2015

[TR-03110_3] Federal Office for Information Security (BSI) 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

[TR-3111] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009

[TR-3116-2] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Stand 2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[UGPre] Guidance Documentation for the Initialization and Personalization Phase ePass Applet on Sm@rtCafé® Expert 8.0 C2, G+D, Version 1.7, 04.08.2023

[UGOpe] Guidance Documentation for the Usage Phase ePass Applet on Sm@rtCafé® Expert 8.0 C2, G+D, Version 0.9, 28.07.2023

[UGOpe-SCE] Operational User Guidance Sm@rtCafé® Expert 8.0 C2, Giesecke+Devrient, Version 2.7, 10.07.2023

[UGPerso] EPASS Applet EPASS10-100 Personalization Concept, Giesecke+Devrient, Version 2.4, 09.03.2023

[UGUsage] EPASS Applet EPASS10-100 Usage Phase Commands, Giesecke+Devrient, Version 1.2, 17.07.2023

[UGMain] Guidance Documentation ePass Applet on Sm@rtCafé® Expert 8.0 C2, Main Document, Giesecke+Devrient, Version 0.7, 28.07.2023

## 9.2 Abbreviations

**API** Application Programming Interface

**BIS** Basic Inspection System

**CAP** Converted Applet

**CC** Common Criteria

**DES** Data Encryption Standard

**DS** Dedicated software

**EAL** Evaluation Assurance Level

**ECC** Elliptic Curve Cryptography

**HW** Hardware

**IC** Integrated Circuit

**IT** Information Technology

**JCRE** Java Card Runtime Environment

**JCVM** Java Card Virtual Machine

**OS** Operating System

**PIN** Personal Identification Number

**PP** Protection Profile

**RAM** Random Access memory

**ROM** Read-Only Memory

**RSA** Rivest, Shamir and Adleman

**SF** Security Function

**SFP** Security Function Policy

**SFR** Security Functional Requirement

**SHA** Secure Hash Algorithm

**ST** Security Target

**SW** Software

**TOE** Target of Evaluation

**TSC** TSF Scope of Control

**TSF** TOE Security Functions

**TSFI** TSF Interface

**TSP** TOE Security Policy

# End of Document