ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0

Security Target

About this document

Scope and purpose

This document contains the Security Target for the evaluation of the **ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0.**

Intended audience

Common Criteria evaluators, Common Criteria certification bodies, Composite product (applet) developers

Table of contents

1 Security Target Introduction (ASE_INT)

1.1 ST Reference

The title of this document is “ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0”.

Version: Rev 1.0

Publication date: 2025-03-21

Sponsor: Infineon Technologies AG, 81726 Munich, Germany

Editor: Infineon Technologies AG, 81726 Munich, Germany

1.2 TOE Reference

The name of the TOE is “ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0” interchangeably called ePass in this ST.

The TOE is a secure chip implementing an ePassport. The TOE is subject to a composite certification based on the Infineon Java Card ‘SECORA™ ID v2.01 (SLJ38Gxymm1ap)’ platform, for details on the latter refer to [ST_JC_Platform].

CC certificate number of underlying Java Card OS Platform: NSCIB-CC-2400062-01

CC certificate number of underlying HW: BSI-DSZ-CC-1169-V4-2024

1.3 TOE Identification

The TOE identification data is as shown in the following table:

Table 1 **TOE identification data**

Topic	**Value**	
TOE release date	24-Sep-2024	
Applet version	1.1.0.0	
TOE version number	2.0	
JC OS Platform related identification data	CC Identifier of underlying hardware platform	IFX_CCI_00005D
	Embedded OS version	CONF1: '01 00 02 FA 15 00 00 13 05' CONF2: '01 00 0C FA 15 00 00 13 05'
	Asymmetric Crypto Library (ACL) version	03.35.001
	Symmetric Crypto Library (SCL) Version	02.15.000
	Hardware Support Library (HSL) Version	03.52.9708
	Hash Crypto Library (HCL) version	01.13.002
	UMSLC version	01.30.0564

The TOE provides a command ‘GET DATA’ with tag 00C1 which provides the release date and the version of the product.

The underlying SECORA™ ID v2.01 (SLJ38Gxymm1ap) platform provides the APDU command "GET TOE Info" which returns the Common Criteria identifier of the platform, the OS version, the specific versions of the cryptographic and hardware support libraries.

The underlying Java Card OS supports two product configurations, such as CONF1 (without In-Field-Update (IFU) Loader feature and CONF2 (with IFU loader feature). The eMRTD delivery covers both the product configurations and based on the customer's request, the required product configuration is chosen during the step 5 described in the chapter 1.6.4.

This ST covers the Java Card OS versions listed in Table 1. Any other Java Card OS version (e.g. loaded using the IFU Loader) is not in the scope of this ST.

1.4 TOE Overview

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by 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).

For the ePassport application, the travel document holder can control access to his user data by conscious presenting his travel document to governmental organisations. The travel document's chip is integrated into a physical (plastic or paper), optically readable part of the travel document, which – as the final product – shall eventually supersede still existing, merely optically readable travel documents. The plastic or paper, optically readable cover of the travel document, where the travel document's chip is embedded in, is not part of the TOE. The tying-up of the travel document's chip to the plastic travel document is achieved by physical and organizational security measures being out of scope of the TOE.

TOE is a Java Card platform with eMRTD application loaded during step 6 Personalisation of Travel Document. All the Java Card OS secure functionalities from [NSCIB-CC-2400062-01] are available to the user during personalization phase. The underlying Java Card OS can be in two possible modes: either in the standard Java Card open mode (loading and installation of applets are possible) or in the proprietary Java Card static mode (preloaded by Infineon packages can be installed, applet loading is not possible).

The TOE comprises at least:

- the circuitry of the MRTD'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 MRTD application and
- the associated guidance documentation.

The preparation of the TOE and its lifecycle is described more detail in chapter 1.6.4.

1.4.2 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_01]) 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.

For this security target the travel document is viewed as unit of:

i. the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder

   a. the biographical data on the biographical data page of the travel document surface,

   b. the printed data in the Machine Readable Zone (MRZ) and

   c. the printed portrait.

ii. the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO_9303_01] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder

   a. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

   b. the digitized portraits (EF.DG2),

   c. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both

   d. the other data according to LDS (EF.DG5 to EF.DG16) and

   e. the Document Security Object (SOD).

1.4.3 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] [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]
- Any product using BAC will be conformant to [PP_BAC] only. Any product using PACE but not using EAC will be conformant to [PP_SAC] only. Any product using PACE and EAC will be conformant to [PP_EAC] only.
- Organizations being responsible for the operation of inspection systems shall be aware of this context.

1.5 Guidance Documentation

The following guidance documentation is delivered to the customer together with the TOE.

Table 2 Guidance Documentation

Document name	Version	Date
ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 Administration Guide	Rev. 1.1	2025-01-28
ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 Extended datasheet	Rev. 1.3	2025-03-19
Additional guidance for Java Card platform with open mode: Underlying OS platform guidances as listed in section 1.4.1.4 of [ST_JC_Platform].		

1.6 TOE Description

1.6.1 Component Overview

The TOE is a DI chip with the ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0. It 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].

Figure 1 shows the TOE in terms of its components.

The green color indicates what contributes to fulfill the security claims in this ST. The white color indicates optional components which are not in the scope of the security claims of this ST, in CC terminology these are non interefering with the TSF of the TOE.

The two lower layers in the picture represent the smart card controller referenced by IFX_CCI_00005D together with the Firmware, Asymmetric Cryptographic Library (ACL) and a Symmetric Crypto Library (SCL). Note that these components are certified by the same CC certificate BSI-DSZ-CC-1169-V4-2024. The hardware platform provides effective protection mechanisms against fault attacks. The platform contains hardware co-processors, which support cryptographic standards such as TDES, AES, RSA and EC. The hardware co-processor SCP has integrated measures against successful SCA.

The OS platform called “SECORA™ ID v2.01 (SLJ38Gxymm1ap)” 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 operations (hash, EC, RSA, TDES and AES)
- Communication via the contactless interface and contact interface.
- It is certified in Common Criteria under the Certificate: NSCIB-CC-2400062-01.

The Java Card OS supports the standard open Java Card mode as well as the proprietary static mode (installation of preloaded code is possible) and the proprietary mode native (specially tailored mode for eMRTD usecase which enforces non traceablity of the TOE). Open and static modes are the two possible modes during personalization of the TOE. The TOE goes into native mode once the personalization is terminated. See [ST_JC_Platform] for more details on the supported modes in the Java Card OS.

ISO or EU Electronic Driving License (eDL) or an Electronic ID (eID) are configurations of SECORA™ ID V2.01 Applet Infineon Applet Collection - eMRTD V2.0. For more information on these optional features refer to [UserGuideDatasheet] and [UserGuideAdmin]. As already said these applications are not part of the TOE Security Functionalities and are non-interfering with the TSFs of the TOE. The installation of eDL and eID is done by the customer who uses the cap file of SECORA™ ID V2.01 Applet Infineon Applet Collection preloaded on the card by Infineon. Again, no claims of the security for the eDL or the eID applications are made in this ST.

Optionally the ISO File SystemV2 applet (here after referred as ISO-FS) can co-exists along with the eMRTD V2.0 applet configurations. The ISO-FS applet provides support to generate file system structures and provide functionalities and commands based on the standards [ISO7816-4], [ISO7816-8] and [ISO7816-9]. The ISO-FS applet is non-interfering with the TSFs of the TOE. No other claims of the security for the ISO-FS applet.

ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 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 is done by the customer who uses for this purpose the cap file of SECORA™ ID v2.01 Applet Infineon Applet Collection preloaded on the card by Infineon.

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 Security Target of ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0.

Third party applications can be installed by the customer and running on the card. Note that in this case the Java Card OS is delivered in open mode, see [ST_JC_Platform] to the customer which will be then able to load and install 3rd party applications.

The TOE user guidance comprises:

[UserGuideDatasheet] and [UserGuideAdmin] which provide guidance, how to perform personalization and maintain the targeted security level during Personalisation and Operation phase. Additionally, when the TOE is delivered with Java Card open mode to load and install the third party applications, the underlying OS platform provides guidance as listed in section 1.4.1.4 of [ST_JC_Platform].

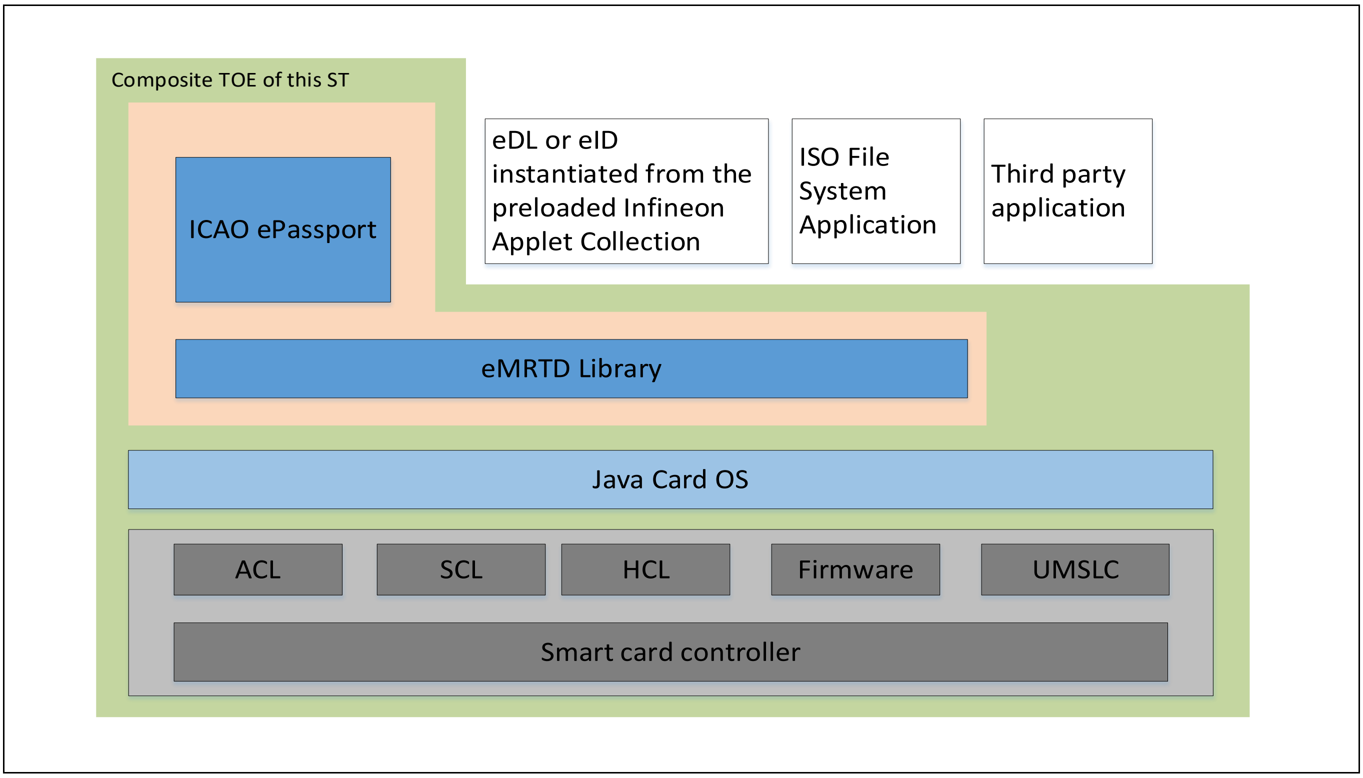

Figure 1 TOE components overview

1.6.2 Interfaces of the TOE

The physical interface of the TOE to the external environment is the entire surface of the IC.

The RF interface (radio frequency power and signal interface) enabling contactless communication between a PICC (proximity integration chip card, PICC) and a terminal reader/writer (proximity coupling device, terminal). The transmission protocol meets [ISO14443-3] and [ISO14443-4].

The contact based interface [ISO7816-3] supported for the purposes of eID and eDL.

The command interface to the TOE is provided by the ePassport Application.

1.6.3 Package Types

The TOE package types and formats are exactly the same as for the underlying Java Card OS. The package types and formats of the Java Card OS are described in [ST_JC_Platform], section 1.4.3 and 1.4.6.

1.6.4 Lifecycle and Delivery

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 of the executable Java Card OS image (either CONF1 or CONF2). Loading of the application JC package containing the TOE code, eDL and eID code. The TOE is delivered to the customer (Step 6) for further personalization of the Travel Document.

3. Personalisation of Travel Document

- Step 6: this step is performed by the customer. The customer receives from Infineon the TOE composed of the following components:
    - The underlying hardware
    - The underlying Java Card OS can be in two possible modes: either in the standard Java Card open mode (loading and installation of applets are possible) or in the proprietary Java Card static mode (preloaded by Infineon packages can be installed, applet loading is not possible).
    - The cap file of ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 is preloaded by Infineon.

The customer then proceeds to installing the ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 and optionally installing the ISO/EU eDL or eID. In case the Java Card OS is in open mode the customer can load and install 3rd party applets. During this step the customer also performs the personalisation with biometric data and configuration of the TSF if necessary.

The TSF data (data created by and for the TOE, that might affect the operation of the TOE; comprise (but are not limited to) the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

The TOE will be set to operational use in Step 7.

4. Operational Use

- Step 7:
    - The TOE is used as MRTD chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or organization and can be used according to the security policy of the issuing State but they can never be modified.
    - The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.
    - Once the personalization of the product is finished, the Java Card OS is switched to its proprietary native mode usage of the TOE by the personalizer. Native mode switches off GP and identification commands to disallow tracking of the end user.

1.6.5 Forms of delivery

The composite TOE is delivered to customers with the deliverey forms mentioned in chapter 1.6.3 via Postal transfer in cages. All materials are delivered to distribution centers in cages, locked.

All User Guidance documents mentioned in chapter 1.5 are delivered as a personalized PDF via webservice portal MyICP.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target and the TOE claim conformance to CC:2022. This ST claims conformance to Common Criteria version CC:2022 revision 1 part 2 [CCPart2] extended and Common Criteria version CC:2022 revision 1 part 3 [CCPart3] conformant. Also conformant to Common Criteria evaluation methods and activities [CEM2022]. [CCErrata] and [CCTrans] are taken into consideration.

2.2 PP Claim

The TOE is strictly conformant to:

- [PP_BAC], if a BIS chooses BAC as authentication method.
- [PP_SAC], if a BIS chooses PACE as authentication method.
- [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].

2.3 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 in case BAC is chosen as authentication method whereby conformancy to [PP_BAC] is claimed.

2.4 Conformance Rationale

With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and [PP_EAC], [PP_SAC] and [PP_BAC], rationales are provided that these changes do not affect the conformance claim to [PP_EAC], [PP_SAC] and [PP_BAC]:

- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 added. Further FCS_CKM.5 is added for key derivation as an alternative.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5. This SFR targets key derivation, subsequent to FCS_CKM.1. In CC:2022 key derivation would have been part of FCS_CKM.1 and thus conformancy to [PP_EAC], [PP_SAC] and [PP_BAC] can still be claimed. FCS_CKM.4 is removed and instead FCS_CKM.6 added. All other dependencies (i.e. FCS_RNG.1 or FCS_RBG.1) are in addition to the already existing ones, i.e. add stricter requirements.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction. As an alternative dependency to FCS_CKM.1, FCS_CKM.5 (key derivation) can be used. As FCS_CKM.5 is neither used within [PP_EAC], [PP_SAC] and [PP_BAC] nor within this ST, it has no relevance in this context.
- FCS_RNG.1: this SFR is taken from [CCPart2] rather than [PP_SAC] and [PP_BAC]. The SFR is refined in [CCPart2].
- FMT_LIM.1 and FMT_LIM.2 in CC:2022 are slightly rephrased (i.e. removing redundancy from FMT_LIM.1) and availability and capability policy mentioned in both SFR's. The meaning though is the same as in [PP_EAC], [PP_SAC] and [PP_BAC] and therefore conformancy can still be claimed.
- FIA_API.1: this SFR is taken from [CCPart2] rather than [PP_EAC]. The SFR requires additional information.

Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to [PP_EAC], [PP_SAC] and [PP_BAC]:

- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for [PP_EAC], [PP_SAC] and [PP_BAC]
- ASE_REQ.2: extended for multi assurance: not relevant for [PP_EAC], [PP_SAC] and [PP_BAC]
- AVA_VAN.5: extension about third party components introduced. No relaxation was introduced.
- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

2.5 Statement of Compatibility

The statement of compatibility is described in the document [SOC].

3 Security Problem Definition (ASE_SPD)

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.

4 Security Objectives (ASE_OBJ)

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

4.1 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.

4.2 Security Objectives defined in this ST

The following security objective is defined additionally in this ST to formally express the extra features of the TOE does 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_01]. The authenticity proof provided by travel document’s chip shall be protected against attacks with high attack potential.

4.3 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 in this ST security objective **OT.Active_Auth** above counters the threat **T.Counterfeit** (threat defined in [PP_EAC].

5 Extended Components Definition (ASE_ECD)

[PP_EAC], [PP_SAC] and [PP_BAC] respective sections 5 "Extended Components Definition" are applicable for this TOE. However, the majority of the SFRs are replaced with SFRs from CC:2022. The mappings and its correspondence are shown in Table 3.

Table 3 Extended SFRs from PP_EAC, PP_SAC and PP_BAC mapped to SFRs in CC:2022

Extended SFRs from PP	Mapping to SFRs in CC:2022	Correspondence
SFRs from [PP_EAC]		
FIA_API.1	FIA_API.1	Replaced and refined with SFR from CC:2022.
FPT_EMS.1	FPT_EMS.1	Replaced and refined with SFR from CC:2022. The SFR from the PP permits to mention the specified limits. However, this is not part of SFR from CC:2022. The SFR from CC:2022 still sufficient to address the practical cases and can be used instead of the SFR from [PP_EAC].
SFRS from [PP_BAC]		
FAU_SAS.1	n.a	Used as is from the PP.
FCS_RND.1	FCS_RNG.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 specifies more details and still fulfils required quality metric details for [PP_BAC].
FMT_LIM.1	FMT_LIM.1	Replaced with SFR from CC:2022. SFRs are identical.
FMT_LIM.2	FMT_LIM.2	Replaced with SFR from CC:2022. SFRs are identical.
FPT_EMSEC.1	FPT_EMS.1	Replaced and refined with SFR from CC:2022. The SFR from the PP permits to mention the specified limits. However, this is not part of SFR from CC:2022. The SFR from CC:2022 still sufficient to address the practical cases and can be used instead of the SFR from [PP_BAC].
FPT_TST.1	FPT_TST.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 additionally specifies the list of self-tests run by the TSF.
SFRS from [PP_SAC]		
FAU_SAS.1	n.a	Used as is from the PP.
FCS_RND.1	FCS_RNG.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 specifies more details and still fulfils required quality metric details for [PP_SAC].
FMT_LIM.1	FMT_LIM.1	Replaced with SFR from CC:2022. SFRs are identical.

Extended SFRs from PP	Mapping to SFRs in CC:2022	Correspondence
FMT_LIM.2	FMT_LIM.2	Replaced with SFR from CC:2022. SFRs are identical.
FPT_EMS.1	FPT_EMS.1	Replaced and refined with SFR from CC:2022. The SFR from the PP permits to mention the specified limits. However, this is not part of SFR from CC:2022. The SFR from CC:2022 still sufficient to address the practical cases and can be used instead of the SFR from [PP_SAC].
FPT_TST.1	FPT_TST.1	Replaced and refined with SFR from CC:2022. The SFR from CC:2022 additionally specifies the list of self-tests run by the TSF.

6 Security Requirements (ASE_REQ)

6.1 TOE Security Functional Requirements

The security functional requirements (SFR) for this TOE are defined in this chapter.
This ST covers the three PPs [PP_EAC], [PP_SAC] 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 4 lists all SFRs appearing both in [PP_SAC] and [PP_BAC].
Table 5 lists all SFRs declared in [PP_SAC].
Table 6 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 7 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 5 and Table 7 are also SFRs of [PP_EAC].
Table 8 lists the SFRs introduced in this ST which are related to the Active Authentication mechanism supported by the TOE.

Operations already performed in the underlying PPs [PP_EAC], [PP_SAC] and [PP_BAC] are marked by underlined font style. Please refer to [PP_EAC], [PP_SAC] and [PP_BAC] for further information on details of the operation.
Operations performed within this Security Target are marked by *italic underlined* font style.

Table 4 TOE SFRs equivalent from both [PP_SAC] and [PP_BAC]

SFRs
FCS_CKM.6
FCS_RNG.1
FMT_MTD.1/INI_ENA
FPT_TST.1
FPT_PHP.3

Note: FCS_CKM.4 is replaced by FCS_CKM.6 in CC:2022.

Note: FCS_RND.1 is refined as FCS_RNG.1 as per CC:2022.

Table 5 TOE SFRs specifically from [PP_SAC]

SFRs
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

SFRs
FDP_ACF.1/TRM
FDP_RIP.1
FDP_UCT.1/TRM
FDP_UIT.1/TRM
FTP_ITC.1/PACE
FAU_SAS.1
FMT_SMF.1
FMT_SMR.1/PACE
FMT_LIM.1
FMT_LIM.2
FMT_MTD.1/INI_DIS
FMT_MTD.1/KEY_READ
FMT_MTD.1/PA
FPT_EMS.1
FPT_FLS.1

Table 6 TOE SFRs specifically from [PP_BAC]

SFRs
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_SMR.1
FMT_LIM.1/BAC
FMT_LIM.2/BAC
FMT_MTD.1/INI_DIS/BAC
FMT_MTD.1/KEY_WRITE

SFRs
FMT_MTD.1/KEY_READ/BAC
FPT_EMS.1
FPT_FLS.1/BAC

Table 7 TOE SFRs specifically from [PP_EAC]

SFRs
FCS_CKM.1/CA
FCS_COP.1/CA_ENC
FCS_COP.1/CA_MAC
FCS_COP.1/SIG_VER
FIA_UID.1/PACE
FIA_UAU.1/PACE
FIA_UAU.4/PACE
FIA_UAU.5/PACE
FIA_UAU.6/EAC
FIA_API.1
FDP_ACC.1/TRM
FDP_ACF.1/TRM
FMT_SMR.1/PACE
FMT_LIM.1
FMT_LIM.2
FMT_MTD.1/CVCA_INI
FMT_MTD.1/DATE
FMT_MTD.1/CAPK
FMT_MTD.1/CVCA_UPD
FMT_MTD.1/KEY_READ
FMT_MTD.3
FPT_EMS.1

Table 8 TOE SFRs introduced in this ST

SFRs
FIA_API.1/AA
FMT_MTD.1/AA
FCS_COP.1/SIG_GEN

6.1.1 About the Application Notes in this ST

Note that if an SFR has application notes as per the PPs [PP_SAC], [PP_EAC] and [PP_BAC] then these application notes apply and can be found in the respective PPs.

Some SFRs contain additional application notes to ease the understanding of the specificities of this TOE. These application notes do not come from the PPs and are prefixed with [IFX specific].

6.1.2 Common SFRs from [PP_BAC] and [PP_SAC]

6.1.2.1 Class FCS: Cryptographic Support

Table 9 FCS_CKM.6

FCS_CKM.6	**Timing and event of cryptographic key destruction – Session keys**
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, or FCS_CKM.5 Cryptographic key derivation]: fulfilled by FCS_CKM.1 in case of BAC; fulfilled by FCS_CKM.1/DH_PACE in case of PACE
FCS_CKM.6.1	The TSF shall destroy *cryptographic keys* when *no longer needed*.
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *overwriting the key values with random values* that meets the following: *none*.
[IFX specific] Application Note:	Application note 19 of [PP_BAC] and application note 28 of [PP_SAC] are both applicable for this SFR. There is no contradiction between the two application notes. While the application note from [PP_BAC] simply requests the encryption and message authentication keys to be destroyed, the application note from [PP_SAC] provides more detailed requests, when the session keys have to be destroyed. Therefore FCS_CKM.4 from [PP_SAC] and [PP_BAC] can be combined and fulfilled using FCS_CKM.6 since FCS_CKM.4 is replaced by FCS_CKM.6 in CC:2022.

Table 10 FCS_RNG.1

FCS_RNG.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a *hybrid physical* random number generator that implements: *Random numbers generation Class PTG.3 according to [AIS31]:* (1) (PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output. (2) (PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*. (3) (PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not

FCS_RNG.1	**Quality metric for random numbers**
	output any random numbers before the power-up online test and the seeding of the DRG.3 postprocessing algorithm have been finished successfully or when a defect has been detected. (4) (PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon. (5) The online test procedure checks the raw random number sequence. It is triggered *continuously*. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time. (6) (PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.
FCS_RNG.1.2	The TSF shall provide *octets of bits* that meet: (1) (PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A. (2) (PTG.3.8) The internal random numbers shall *use PTRNG of class PTG.2 as random source for the post-processing*.
[IFX specific] Application Note:	There is no contradiction between application note 24 of [PP_BAC] and application note 31 of [PP_SAC]. Both application notes shall apply and therefore FCS_RND.1 from [PP_BAC] and [PP_SAC] can be combined, i.e. the random numbers shall be used for the PACE, BAC and the authentication mechanism based on Triple-DES (as defined in FIA_UAU.4/PACE and FIA_UAU.4). The FCS_RND.1 is refined as FCS_RNG.1 from CC:2022. Still the refined SFR meets [PP_BAC] and [PP_SAC].

6.1.2.2 Class FMT Security Management

Table 11 FMT_MTD.1/INI_ENA

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 for PACE; fulfilled by FMT_SMF.1/BAC for BAC FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE for PACE; fulfilled by FMT_SMR.1 for BAC.
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to *write* the *Initialisation Data and Prepersonalisation Data* to *the Manufacturer*.
[IFX specific] Application Note:	The application note 42 of [PP_BAC] applies. This application note provides a definition, what is meant by “Pre-Personalisation Data”. This definition is also applicable to FMT_MTD.1/INI_ENA from [PP_SAC]. Therefore FMT_MTD.1/INI_ENA from [PP_BAC] and [PP_SAC] can be combined.

6.1.2.3 Class FPT Protection of the Security Functions

Table 12 FPT_TST.1

FPT_TST.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of following self tests *during initial start-up*, to demonstrate the correct operation of the TSF: *the Java Card OS the UMSLC (User Mode Security Life Control) selftest offered by the hardware platform is performed*.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.
[IFX specific] Application Note:	There is no contradiction between application note 46 of [PP_BAC] and application note 52 of [PP_SAC]. In fact, although the wording is slightly different, the meaning of these application notes is identical. Therefore, either of these application notes applies and FPT_TST.1 from [PP_BAC] and [PP_SAC] can be combined.

Table 13 FPT_PHP.3

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 to the TSF by responding automatically such that the SFRs are always enforced.
[IFX specific] Application Note:	Application note 47 of [PP_BAC] and 53 of [PP_SAC] are equivalent. Application note 48 of [PP_BAC] is only informative to the reader in the sense, that it provides a context to an older CC standard, but not relevant for the interpretation of FPT_PHP.3. Therefore, either application note 47 of [PP_BAC] or application note 53 of [PP_SAC] applies and FPT_PHP.3 from [PP_BAC] and [PP_SAC] can be combined.

6.1.3 SFRs specifically from [PP_SAC]

6.1.3.1 Class FCS: Cryptographic Support

Table 14 FCS_CKM.1/DH_PACE

FCS_CKM.1/DH_PACE	**Cryptographic key generation – Diffie-Hellman for PACE session keys**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.6

FCS_CKM.1/DH_PACE	**Cryptographic key generation – Diffie-Hellman for PACE session keys**
	Justification: A ECDH agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case while FCS_CKM.6 Timing and event of cryptographic key destruction makes sense. [FCS_RBG.1 Random bit generation or FCS_RNG.1 Generation of random numbers]: fulfilled by FCS_RNG.1
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_ECC]* and specified cryptographic key sizes *Table 15 column key size* that meet the following: [ICAO_SAC].

Table 15 FCS_CKM/DH_PACE Key Sizes

Algorithm	**Key size**
ECDH key agreement algorithm	192, 224, 256, 320, 384, 512, 521
AES session keys	128, 192, 256
TDES session keys	112

Table 16 FCS_COP.1/PACE_ENC

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, or FCS_CKM.5 Cryptographic key derivation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.6 Timing and event of cryptographic key destruction: fulfilled by FCS_CKM.6.
FCS_COP.1.1/PACE_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *AES and 3DES* in CBC mode and cryptographic key sizes *128, 192 and 256 bits for AES and 112 bits for 3DES* that meet the following: compliant to [ICAO_SAC].
[IFX specific] Application Note:	3DES in CBC mode is used with key size of 112 bit. AES in CBC mode is used with key size of 128, 192 or 256 bits. The 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.

Table 17 FCS_COP.1/PACE_MAC

FCS_COP.1/PACE_MAC	**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

FCS_COP.1/PACE_MAC	**MAC Cryptographic operation – MAC**
	key generation, or FCS_CKM.5 Cryptographic key derivation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.6 Timing and event of cryptographic key destruction: fulfilled by FCS_CKM.6.
FCS_COP.1.1/PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *CMAC and Retail-MAC* and cryptographic key sizes *112, 128, 192, 256* bit that meet the following: compliant to [ICAO_SAC].
[IFX specific] Application Note:	In accordance with [ICAO_SAC] the (two-key) Triple-DES (112 Bit) could be used in Retail mode for secure messaging.

6.1.3.2 Class FIA Identification and Authentication

Table 18 FIA_AFL.1/PACE

FIA_AFL.1/PACE	**Authentication failure handling – PACE authentication using non-blocking authorisation data**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when *a configurable number (see application note below)* of unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall *increasingly slow down the performance up to a maximum a configurable number (see application note below) verifying the authentication token*.
[IFX specific] Application Note:	The delay counter to increasingly slow down the performance is configurable. This configurable number can be in the range [0x01 to 0x7F]. The number of failed authentication attempts is configurable. This configurable number can be in the range [0x01 to 0x7F].

Table 19 FIA_UID.1/PACE

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 a communication channel, 2. carry 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* on behalf of the user to be performed before the user is identified.

FIA_UID.1/PACE	**Timing of identification**
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.

Table 20 FIA_UAU.1/PACE

FIA_UAU.1/PACE	**Timing of authentication**
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 a 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* 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.

Table 21 FIA_UAU.4/PACE

FIA_UAU.4/PACE	**Single-use authentication of the Terminals 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 *Triple-DES and AES* *3. none*

Table 22 FIA_UAU.5/PACE

FIA_UAU.5/PACE	**Multiple authentication mechanisms**
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 [ICAO_9303_01] 3. Secure messaging in MAC-ENC mode according to [ICAO_SAC] 4. Symmetric Authentication Mechanism based on *secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length* *5. none* to support user authentication.
FIA_UAU.5.2/PACE	The TSF shall authenticate any user's claimed identity according to the following rules:

FIA_UAU.5/PACE	Multiple authentication mechanisms
	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 *secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length*. *3. none*
[IFX specific] Application Note:	This SFR also specifies the means for authentication of the personalization agent that are used during personalization phase which are the scp03 as per [GPv2_3_1], see point 2 of FIA_UAU.5.2/PACE above.

Table 23 FIA_UAU.6/PACE

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

6.1.3.3 Class FDP User Data Protection

Table 24 FDP_ACC.1/TRM

FDP_ACC.1/TRM	Subset access control – Terminal Access
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 on terminals gaining access to the User Data stored in the travel document and *EF.SOD*.
Application note:	Please note that the Document Security Object (SOD) stored in EF.SOD (see [ICAO_9303_01]) 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 [ICAO_9303_01].

Table 25 FDP_ACF.1/TRM

FDP_ACF.1/TRM	Subset access control – Terminal Access
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM FMT_MSA.3 Static attribute initialisation: not fulfilled but justified. The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation and fixed over the whole lifetime of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

FDP_ACF.1/TRM	**Subset access control – Terminal Access**
FDP_ACF.1.1/TRM	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE; 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 *4. none*
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. A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [ICAO_SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*
FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional 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*

Table 26 FDP_RIP.1

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 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 ECDH shared secret K), *3. none*

Table 27 FDP_UCT.1/TRM

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 to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

Table 28 FDP_UIT.1/TRM

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

6.1.3.4 Class FTP Trusted Path/Channels

Table 29 FTP_ITC.1/PACE

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.

6.1.3.5 Class FAU Security Audit

Table 30 FAU_SAS.1

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FAU_SAS.1	Audit storage
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records.

6.1.3.6 Class FMT Security Management

Table 31 FMT_SMF.1

FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSFshall be capable of performing the following management functions: 1. Initialization, 2. Pre-personalisation, 3. Personalisation, 4. Configuration.

Table 32 FMT_SMR.1

FMT_SMR.1	Security roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1/PACE	The TSFshall maintain the roles 1. Manufacturer, 2. Personalisation Agent, 3. Terminal, 4. PACE authenticated BIS-PACE. *5. None*
FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.

Table 33 FMT_LIM.1

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/PACE	The TSF shall limit its capabilities so that in conjunction with 'Limited availability (FMT_LIM.2) the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, *4.* substantial information about construction of TSF to be gathered which may enable other attacks

Table 34 FMT_LIM.2

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.
FMT_LIM.2.1/PACE	The TSF shall be designed in a manner that limits its availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, *4.* substantial information about construction of TSF to be gathered which may enable other attacks

Table 35 FMT_MTD.1/INI_DIS

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 the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.

Table 36 FMT_MTD.1/KEY_READ

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 the 1. PACE passwords, 2. Personalisation Agent Keys *3.* *none* to *none*

Table 37 FMT_MTD.1/PA

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 the Document Security Object (SO_D) to the Personalisation Agent.

6.1.3.7 Class FPT Protection of the Security Functions

Table 38 FPT_EMS.1

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 39.

Table 39 FPT_EMS1.1 Emanation of TSF and User data

ID	Emissions	Attack surface	TSF data	User data
1	Electromagnetic and current emissions	contactless/contact interface and circuit contacts	• PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}) • the ephemeral private key ephem-SK_{PICC}-PACE	*none*

Table 40 FPT_FLS.1

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*

6.1.4 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”.

6.1.4.1 Class FCS: Cryptographic Support

Table 41 FCS_CKM.1

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_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation or FCS_RNG.1 Generation of random numbers]: fulfilled by FCS_RNG.1 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1	**Cryptographic key generation – Generation of Document Basic Access Keys by the TOE**
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 and specified cryptographic key sizes 112 bit that meet the following: [ICAO_9303_01], normative appendix 5.

Table 42 FCS_COP.1/SHA

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm *SHA-1* and cryptographic key sizes none that meet the following: *[NIST_Hash]*

Table 43 FCS_COP.1/ENC

FCS_COP.1/ENC	**Cryptographic operation – 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bit that meet the following: [NIST_DES] and [ICAO_9303_01]; normative appendix 5, A 5.3

Table 44 FCS_COP.1/AUTH

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption in accordance with a specified cryptographic algorithm AES and cryptographic key sizes *256 bits* that meet the following: [FIPS_197].

Table 45 FCS_COP.1/MAC

FCS_COP.1/MAC	**Cryptographic operation – Retail MAC**
Hierarchical to:	No other components.

FCS_COP.1/MAC	Cryptographic operation – Retail MAC
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Importof user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bit that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)

6.1.4.2 Class FIA Identification and Authentication

Table 46 FIA_UID.1

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 the random identifier in Phase 3 “Personalisation of the MRTD”, 3. to read the random identifier in Phase 4 “Operational Use” 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.

Table 47 FIA_UAU.1

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 “Personalisation of the MRTD”, 3. to read the random identifier in Phase 4 “Operational Use” 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.

Table 48 FIA_UAU.4

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	**Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Authentication Mechanism based on *Triple-DES and AES.*

Table 49 FIA_UAU.5

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 *secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length* 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 Personalisation Agent by one of the following mechanism(s): *the Symmetric Authentication Mechanism based on scp03 AES 256 bits key length with the Personalisation Agent Key.* 2. the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
[IFX specific] Application Note:	This SFR also specifies the means for authentication of the personalization agent that are used during personalization phase which are the scp03 as per [GPv2_3_1], see point 2 of FIA_UAU.5.2/PACE above.

Table 50 FIA_UAU.6

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

Table 51 FIA_AFL.1

FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_AFL.1.1	The TSF shall detect when *a configurable number (see application note below) of* unsuccessful authentication attempts occur related to *authentication attempts using the BAC password as shared password.*
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met* the TSF shall *increasingly slow down the performance up to a*

FIA_AFL.1	**Authentication failure handling**
	maximum a configurable number (see application note below) verifying the authentication token.
[IFX specific] Application note	The number of failed authentication attempts is configurable. This configurable number can be in the range [0x01 to 0x7F]. The delay counter to increasingly slow down the performance is configurable. This configurable number can be in the range [0x01 to 0x7F].

6.1.4.3 Class FDP User Data Protection

Table 52 FDP_ACC.1

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 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.

Table 53 FDP_ACF.1

FDP_ACF.1	**Basic 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 to objects based on the following: 1. Subjects: a. Personalisation Agent, b. Basic Inspection System, c. Terminal, 2. Objects a. data EF.DG1 to EF.DG16 of the logical MRTD, b. data in EF.COM, c. data in EF.SOD, 3. Security attributes a. authentication status of terminals
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 Personalisation 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.

FDP_ACF.1	**Basic Security attribute based access control – Basic Access Control**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
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. ~~The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.~~
Refinement:	This SFR was refined (deletion of 3. from the list of Objects) as the optional EF.DG3 and EF.DG4 are not created and therefore do not exist.

Table 54 FDP_UCT.1

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 to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

Table 55 FDP_UIT.1

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

6.1.4.4 Class FAU Security Audit

Table 56 FAU_SAS.1/BAC

FAU_SAS.1/BAC	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1/BAC	The TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records.

6.1.4.5 Class FMT Security Management

Table 57 FMT_SMF.1/BAC

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-Personalisation, 3. Personalisation.

Table 58 FMT_SMR.1/BAC

FMT_SMR.1/BAC	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1/BAC	The TSF shall maintain the roles 1. Manufacturer, 2. Personalisation Agent, 3. Basic Inspection System
FMT_SMR.1.2/BAC	The TSF shall be able to associate users with roles.

Table 59 FMT_LIM.1/BAC

FMT_LIM.1/BAC	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2
FMT_LIM.1.1 /BAC	The TSF shall limit its 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

Table 60 FMT_LIM.2/BAC

FMT_LIM.2/BAC	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1.
FMT_LIM.2.1 /BAC	The TSF shall be designed in a manner that limits its availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery do not allow

FMT_LIM.2/BAC	Limited availability
	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

Table 61 FMT_MTD.1/INI_DIS/BAC

FMT_MTD.1/INI_DIS/BAC	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/BAC	The TSF shall restrict the ability to disable read access for users to the Initialisation Data to the Personalisation Agent.

Table 62 FMT_MTD.1/KEY_WRITE

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 the Document Basic Access Keys to the Personalisation Agent.

Table 63 FMT_MTD.1/KEY_READ/BAC

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 fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/KEY_READ/BAC	The TSF shall restrict the ability to read the Document Basic Access Keys and Personalisation Agent Keys to none.

6.1.4.6 Class FPT Protection of the Security Functions

Table 64 FPT_EMS.1

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMS.1.1	The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 65.

Table 65 FPT_EMS1.1 Emanation of TSF and User data

ID	Emissions	Attack surface	TSF data	User data
1	Electromagnetic and current emissions	smart card circuit contacts	• Personalisation Agent Key(s) • Document Basic Access Keys	*none*

Table 66 FPT_FLS.1/BAC

FPT_FLS.1/BAC	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 out-of-range operating conditions where therefore a malfunction could occur, 2. Failure detected by TSF according to FPT_TST.1,

6.1.5 SFRs specifically from [PP_EAC]

6.1.5.1 Cryptographic support

Table 67 FCS_CKM.1/CA

FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation or FCS_RNG.1 Generation of random numbers]: fulfilled by FCS_RNG.1
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH cryptographic key generation algorithm* and specified cryptographic key sizes: *id-CA-ECDH-3DES-CBC-CBC 112 bits,* *id-CA-ECDH-AES-CBC-CMAC-128 128 bits,* *id-CA-ECDH-AES-CBC-CMAC-192 192 bits,* *id-CA-ECDH-AES-CBC-CMAC-256 256 bits* that meet the following: *ECDH protocol compliant to [TR_ECC]*.

6.1.5.2 Cryptographic operations

Table 68 FCS_COP.1/CA_ENC

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/CA_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm *AES and 3DES in CBC mode* and cryptographic key sizes *112, 128, 192 and 256 bit* that meet the following: *compliant to [TR_03110_1]*[TR_03110_1].
[IFX specific] Application note	Personalisation of the TOE is done using the secure channel protocol scp 03 as specified in [GPv2_3_1] with AES 256 bits key length with command encryption compliant with NIST 800-38A.

Table 69 FCS_COP.1/SIG_VER

FCS_COP.1/SIG_VER	**Cryptographic operation – Signature verification by travel document**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes: *id-TA-ECDSA-SHA1 192 bits,* *id-TA-ECDSA-SHA224 224, 256, 320, 384, 512 and 521 bits,* *id-TA-ECDSA-SHA256 256, 320, 384, 512 and 521 bits,* *id-TA-ECDSA-SHA384, 384, 512 and 521 bits,* *id-TA-ECDSA-SHA512, 512 and 521 bits* that meet the following: *[TR_03110_1].*

Table 70 FCS_COP.1/SIG_GEN

FCS_COP.1/SIG_GEN	**Cryptographic operation – Signature generation by MRTD (AA)**
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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/SIG_GEN	The TSF shall perform digital signature generation in accordance with a specified cryptographic algorithm: *RSA based Digital Signature scheme 1 with SHA1, SHA224, SHA256, SHA384 or SHA512 with RSA CRT 1024 to 4096 key length bits* *or*

FCS_COP.1/SIG_GEN	Cryptographic operation – Signature generation by MRTD (AA)
	ECDSA with SHA1, SHA224, SHA256, SHA384 or SHA512 and cryptographic key sizes of 192, 224, 256, 320, 384, 512 or 521 bits; that meet the following: *[ISO9796-2] for RSA signatures and [TR_03110_1] for ECDSA.*
[IFXspecific] Application Note:	The TOE performs digital signature generation with RSA or ECDSA. This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in section 2.2. The digital signature creation is necessary to allow Active Authentication (AA). This extension does not conflict with the strict conformance to the claimed Protection Profiles.

Table 71 FCS_COP.1/CA_MAC

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm *AES CMAC and 3DES-CBC* and cryptographic key sizes *128, 192, 256 bits for AES CMAC and 112 for 3DES-CBC* that meet the following: *compliant to [ICAO_SAC]*.
[IFX specific] Application note	Personalisation of the TOE is done using the secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length with CMAC compliant with NIST 800-38A.

6.1.5.3 Class FIA Identification and Authentication

The following table provides an overview of the authentication mechanisms used.

Table 72 Authentication mechanims

Name	SFR for the TOE
Authentication Mechanism for Personalisation Agents	FIA_UAU.4/PACE
Chip authentication v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Chip Active Authentication	FIA_API.1/AA
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol (listed only for information purposes, so will not be described further in this section)	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive authentication	FIA_UAU.5/PACE

Table 73 FIA_API.1/AA

FIA_API.1/AA	Authentication Proof of Identity (Active Authentication)
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/AA	The TSF shall provide *the Active Authentication Mechanisms according to [ICAO_9303_01]* to prove the identity of the *TOE* by including the following properties *proof of knowledge of administrator credentials* to an external entity.
[IFX specific] Application Note:	The SFR FIA_API.1/AA has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in section 3.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

Table 74 FIA_UID.1/PACE

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. to carry out the Chip Authentication Protocol v.1 according to [TR_03110_1] 5. to carry out the Terminal Authentication Protocol v.1 according to [TR_03110_1] (see next item 6) *6. to carry out the Active Authentication Mechanism* on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Table 75 FIA_UAU.1/PACE

FIA_UAU.1/PACE	Timing of authentication
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
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 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] (see next item 7) *7. to carry out the Active Authentication Mechanism*

FIA_UAU.1/PACE	**Timing of authentication**
	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.

Table 76 FIA_UAU.4/PACE

FIA_UAU.4/PACE	**Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according [ICAO_SAC], 2. Authentication Mechanism based on *Triple- DES or AES*. 3. Terminal Authentication Protocol v.1 according to [TR_03110_1].

Table 77 FIA_UAU.5/PACE

FIA_UAU.5/PACE	**Multiple authentication mechanisms**
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 [ICAO_9303_01], 3. Secure messaging in MAC-ENC mode according to [ICAO_SAC], 4. Symmetric Authentication Mechanism based on *secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length* 5. Terminal Authentication Protocol v.1 according to [TR_03110_1], 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 *secure channel protocol 03 as specified in [GPv2_3_1] with AES 256 bits key length.* 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1. 4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 19. *5. None*

FIA_UAU.5/PACE	**Multiple authentication mechanisms**
[IFX specific] Application Note:	This SFR also specifies the means for authentication of the personalization agent that are used during personalization phase which are the scp03 as per [GPv2_3_1], see point 2 of FIA_UAU.5.2/PACE above.

Table 78 FIA_UAU.6/EAC

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.

Table 79 FIA_API.1

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR_03110_1] to prove the identity of *the TOE* by including the following properties *proof of knowledge of administrator credentials* to an external entity.

6.1.5.4 Class User Data Protection

Table 80 FDP_ACC.1/TRM

FDP_ACC.1/TRM	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/TRM	The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document

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

Table 81 FDP_ACF.1/TRM

FDP_ACF.1/TRM	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access controlFMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/TRM	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE c. Extended Inspection System 2. Objects:

FDP_ACF.1/TRM	Security attribute based access control
	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, d. all TOE intrinsic secret cryptographic keys stored in the travel document 3. Security attributes: a. PACE Authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal.
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.
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/TRM	The TSF shall explicitly deny access of subjects to objects based on the following additional 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. 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.

6.1.5.5 Class FMT Security Management

Table 82 FMT_SMR.1/PACE

FMT_SMR.1/PACE	Security roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1/PACE	The TSF shall maintain the roles 1.Manufacturer ,

FMT_SMR.1/PACE	**Security roles**
	2.Personalisation 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.
FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.

Table 83 FMT_LIM.1

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow, 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.

Table 84 FMT_LIM.2

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow: 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.

Table 85 FMT_MTD.1/CVCA_INI

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/CVCA_INI	**Management of TSF data – Initialization of CVCA Certificate and Current Date**
FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date, *4. none* to *Personalisation agent*.

Table 86 FMT_MTD.1/CVCA_UPD

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

Table 87 FMT_MTD.1/DATE

FMT_MTD.1/DATE	**Management of TSF data – Current date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functionsFMT_SMR.1 Security roles
FMT_MTD.1.1/DATE	The TSF shall restrict the ability to modify the Current date to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System.

Table 88 FMT_MTD.1/CAPK

FMT_MTD.1/CAPK	**Management of TSF data – Chip Authentication Private Key**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles
FMT_MTD.1.1/CAPK	The TSF shall restrict the ability to *load* the Chip Authentication Private Key to *Personalisation agent*.

Table 89 FMT_MTD.1/KEY_READ

FMT_MTD.1/KEY_READ	**Management of TSF data – Key Read**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functionsFMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read the 1. PACE passwords, 2. Chip Authentication Private Key,

FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
	3. Personalisation Agent Keys to *none*.

Table 90 FMT_MTD.3

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.
Refinement:	The certificate chain is valid if and only if 1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE, 2. the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE, 3. the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE. The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System. 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.

Table 91 FMT_MTD.1/AA Management of TSF data

FMT_MTD.1/AA Management of TSF data	**Active Authentication Private Key**
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/AA	The TSF shall restrict the ability to *create and load the Active Authentication Private Key* to *the Manufacturer and the Personalisation Agent*.
[IFX specific] Application Note:	This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in section 3.2 to address the import of private key used for AA. This extension does not conflict with the strict conformance to the claimed Protection Profiles

6.1.5.6 Class FPT Protection of the Security Functions

Table 92 FPT_EMS.1

FPT_EMS.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMS.1.1	The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 93.

Table 93 FPT_EMS1.1 Emanation of TSF and User data

ID	Emissions	Attack surface	TSF data	User data
1	variations in power consumption or timing during command execution	interface smart card circuit contacts	• Chip Authentication Session Keys • PACE Session Keys (PACE-K MAC, PACE-KEnc), • the ephemeral private key ephem SK PICC-PACE, • Personalisation Agent Key(s) • Chip Authentication Private Key • Active Authentication Private Key.	*none*

6.2 Security Assurance Requirements

For the BAC feature, the TOE claims EAL 4 augmented with ALC_DVS.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.

6.3 Security Requirements Rationale

6.3.1 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/AA and FCS_COP.1/SIG_GEN formalizing the Active Authentication feature they meet the security objective OT.Active_Auth.

6.3.2 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.

Table 94 Rationale for SFR's Dependencies (SFRs introduced in this ST)

SFR	Dependencies	Support of the Dependencies
FIA_API.1/AA	No dependencies.	n.a
FMT_MTD.1/AA	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE	Fulfilled by FMT_SMF.1 and FMT_SMR.1/PACE
FCS_COP.1/SIG_GEN	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	Fulfilled by FCS_CKM.1 and FCS_CKM.6

6.3.3 Security Assurance Requirements Rationale

[PP_BAC] section 6.3.3 "Security Assurance Requirements Rationale" is applicable for this chapter.

[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.

6.3.4 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 6.3.3 "Security Assurance Requirements Rationale" together with the additional rational from section 6.3.3 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.

7 TOE Summary Specification

This TOE summary specification described in this section relies on the security services provided by the platform product. For a description of these services please refer to [ST_JC_Platform].

In the following each SFR is mentioned together with an indication for the PP from which these are originating

- (BAC) stands for SFRs originating from [PP_BAC].
- (SAC) stands for SFRs originating from [PP_SAC].
- (EAC) stands for SFRs originating from [PP_EAC]. Note that we include here also in this group the SFRs related to Active Authentication.

The composite TOE provides the security functions as follows:

SF_EAC_PACE_BAC

The TOE implements the EAC, PACE and BAC protocol (PICC side). It encompasses:

- ECDH key generation, **FCS_CKM.1/DH_PACE** (SAC) and **FCS_CKM.1/CA** (EAC): The TOE uses the platform service “Elliptic Curves EC” for EC key generation. Further for session key generation the application uses the hybrid physical random number generator of the platform complying to PTG.3 as per [AIS31]. For the key generation the TOE supports “Generic Mapping” provided by the platform.
- Generation of Document Basic Access Keys, **FCS_CKM.1** (BAC), **FCS_COP.1/SHA** (BAC): The TOE uses the cryptographic APIs provided by the underlying Java Card OS.
- Timing and event of cryptographic key destruction, **FCS_CKM.6**: The TOE uses the platform API ‘clearKey’ service to destroy session keys. The platform API ‘clearKey’ uses random numbers compliant to PTG.3 as per [AIS31] to overwrite the session keys.
- Provision of random numbers, as per **FCS_RNG.1**. Authentication failure handling, **FIA_AFL.1/PACE** (SAC), **FIA_AFL.1** (BAC): The TOE implements this check in such a way, that it withstands tearing events. A counter for unsuccessful authentication attempts is incremented before authentication is performed and reset in case of successful authentication.
- Prevention of replay attacks, **FIA_UAU.4/PACE** (EAC), **FIA_UAU.4/PACE** (SAC), **FIA_UAU.4** (BAC): Replay attacks are prevented by the cryptographic protocol, which relies on good quality random numbers as required by FCS_RNG.1 of this ST and supported by the underlying RNG of the platform and claimed in the ST of the platform with SFR FCS_RNG.1.
- Multiple authentication, **FIA_UAU.5/PACE** (EAC), **FIA_UAU.5/PACE** (SAC), **FIA_UAU.5** (BAC): The TOE follows the protocol as described in [ICAO_SAC].

SF_AA

- Signature generation for the Active Authentication mechanism covered by **FIA_API.1/AA, FCS_COP.1/SIG_GEN**
- Injecting private cryptographic keys used for the signatures as per **FMT_MTD.1/AA**

SF_AuthPersoAgent

- **FIA_UAU.5/PACE** (EAC), **FIA_UAU.5/PACE** (SAC), **FCS_COP.1/AUTH** (BAC): The TOE uses the protocol scp v0.3 as per [GPv2_3_1] based on AES [FIPS_197] for authenticating the personalization agent.

SF_SecureMessaging

- Secure messaging, encryption/decryption, **FCS_COP.1/PACE_ENC** (SAC), **FCS_COP.1/ENC** (BAC): The TOE uses the proprietary PACE API from Java Card OS.
- Secure messaging integrity protection, **FCS_COP.1/PACE_MAC** (SAC), **FCS_COP.1/MAC** (BAC): The TOE uses the underlying platform PACE dedicated API to calculate CMAC or Retail-MAC.
- **FCS_COP.1/CA_ENC** (EAC), **FCS_COP.1/CA_MAC** (EAC) and **FCS_COP.1/SIG_VER** (EAC) are satisfied by using the standard Java Card API supported by the platform.
- **FCS_COP.1/CA_MAC** (EAC) also covers to the GP scp03 used for secure card content management during personalization. This aspect of secure messaging by the TOE relies on the specially tailored API to GP SCP from the underlying platform and described in the SFR FCS_COP.1/SCP.
- Multiple authentication, **FIA_UAU.5/PACE** (SAC), **FIA_UAU.5** (BAC): The TOE performs a MAC check for every received message before instruction is executed, if the MAC check fails secure messaging is aborted; every response during secure messaging is MAC'ed by the TOE.
- Re-authentication of terminal, **FIA_UAU.6/EAC** (EAC), **FIA_UAU.6/PACE** (SAC), **FIA_UAU.6** (BAC): The TOE checks for every incoming message, whether the message is genuine (MAC check).
- Trusted channel, **FTP_ITC.1/PACE** (SAC): The TOE follows the standardized implementation of the trusted channel according to [ICAO_SAC].

SF_AccessControl

- Allow specific access before user identification, **FIA_UID.1/PACE** (EAC), **FIA_UID.1/PACE** (SAC), **FIA_UID.1** (BAC): The access rights information of the TOE grant access to EF.CardAccess (see [ICAO_9303_11]) and EF.ATR/INFO (see [ISO7816-4]) before PACE or BAC authentication is performed. The TOE allows to read a specific subset of initialization data.
- Allow specific access before user authentication, **FIA_UAU.1/PACE** (EAC), **FIA_UAU.1/PACE** (SAC), **FIA_UAU.1** (BAC): The access rights information of the TOE grant access to EF.CardAccess and EF.ATR/INFO before PACE or BAC authentication was performed. The TOE allows to read a specific subset of initialization data.
- Subset and security attribute based access control, **FDP_ACC.1/TRM** (EAC), FDP_ACC.1/TRM (SAC), **FDP_ACC.1** (BAC), **FDP_ACF.1/TRM** (EAC), **FDP_ACF.1/TRM** (SAC), **FDP_ACF.1** (BAC), the TOE blocks access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM, EF.DG3 and EF.DG4 in case BAC or PACE protocol is not successfully performed.
- Residual information protection, **FDP_RIP.1**: as soon secure messaging is stopped, the whole secure messaging context including session keys is wiped with random numbers.
- Data exchange confidentiality, **FDP_UCT.1/TRM** (SAC), **FDP_UCT.1** (BAC): during secure messaging, responses by the ICC are always wrapped (encrypted and MAC'ed) before being sent.
- Data exchange integrity, **FDP_UIT.1/TRM** (SAC), **FDP_UIT.1** (BAC) : during secure messaging, responses by the ICC are always wrapped (encrypted and MAC'ed) before being sent. A MAC check is performed for each message received during secure messaging.
- Storage of initialization and pre-personalisation data, **FAU_SAS.1** (SAC), **FAU_SAS.1/BAC** (BAC): [PP_BAC] requests storage of IC Identification data, whereas [PP_SAC] requests storage of Initialisation and Pre-Personalisation data, whereby IC Identification data is a subset of Initialisation data. The TOE does not make any distinction, whether BAC or PACE is performed, i.e. stores all of the requested data. The TOE at its stage of delivery (Personalisation stage) contains a Personalisation key. The Personalisation agent has the option to calculate various checksums including software, file system, chip information and lifecycle information.

- Management functions linked to different life cycle states, **FMT_SMF.1** (SAC), **FMT_SMF.1/BAC** (BAC): The management functions "Initialization" and "pre-Personalisation" are part of the developer lifecycle.

- Access is linked to security roles, **FMT_SMR.1/PACE** (EAC), **FMT_SMR.1/PACE** (SAC), **FMT_SMR.1** (BAC): Access rights are implemented such, that they depend on lifecycle stage and authentication stage (e.g. whether PACE authentication or authentication as Personalisation agent was successfully performed). Certain commands are blocked during specific lifecycle states, such as the command to read the Initialisation data or update file data in operation state. Read access to specific files is granted or denied depending on the authentication state. Life cycle transition from Personalisation to operation stage can only be performed by the Personalisation agent. A back transition is blocked.

- Writing of initialization and pre-personalisation data restricted to manufacturer, **FMT_MTD.1/INI_ENA**: during Personalisation and operation there is no command available to write initialization data (e.g. create files). Card manager keys can be updated in personalization phase. Note that personalization keys are the card manager/ issuer security domain key and therefore are not owned by the applet.

- Reading of initialization and pre-personalisation data restricted to Personalisation agent, **FMT_MTD.1/INI_DIS** (SAC) and Disabling of Read Access to Initialization Data to the Personalisation agent **FMT_MTD.1/INI_DIS/BAC** (BAC): Although these two SFRs have slightly different meanings, the TOE generally blocks reading of initialization and pre-Personalisation data in operation mode. Only the Personalisation agent is granted to set the lifecycle state from Personalisation to operation. A back transition is blocked.

- Reading of EAC, PACE or BAC keys and Personalisation agent key not possible, **FMT_MTD.1/KEY_READ** (EAC), **FMT_MTD.1/KEY_READ** (SAC), **FMT_MTD.1/KEY_READ/BAC** (BAC): The Personalisation key, PACE passwords, Document Basic Access Keys for BAC, Chip Authentication Private Key for EAC are stored in a special key storage within the platform, which only allows to handle this key by reference; no read access is performed by the application.

- Only Personalisation agent allowed to write Document Security Object (SOD), **FMT_MTD.1/PA**: In operation mode the "STORE DATA" command is blocked.

- Only Personalisation agent allowed to write Document Basic Access Keys, **FMT_MTD.1/KEY_WRITE** (BAC): in operation stage the proprietary command to write Document Basic Access Keys is blocked.

- **FMT_MTD.1/CVCA_INI** (EAC)requires that the TSF shall restrict the ability to write the initial Country Verifying Certification Authority Public Key, the   initial Country Verifying Certification Authority Certificate, and the initial Current Date to the Personalization Agent. Access over to this data is a subject to an access control.

- **FMT_MTD.1/CVCA_UPD** (EAC)requires that the TSF shall restrict the ability to update the Country Verifying Certification Authority Public Key and the Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. **SF_AccessControl** realizes the appropriate control over the access rights.

- **FMT_MTD.1/DATE** (EAC)requires that the TSF shall restrict the ability to modify the Current date to the Country Verifying Certification Authority, the Document Verifier, and the Domestic Extended Inspection System. **SF_AccessControl** realizes the appropriate control over the access rights.

- **FMT_MTD.1/CAPK** (EAC)requires that the TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent. **SF_AccessControl** realizes the appropriate control over the access rights.

- **FMT_MTD.3** (EAC) that the TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control as described in the refinement of the SFR.

SF_DataProtection

- TSF is designed, that it has limited capability and limited availability, **FMT_LIM.1** (EAC), **FMT_LIM.2** (EAC), **FMT_LIM.1** (SAC), **FMT_LIM.1/BAC** (BAC), **FMT_LIM.2** (SAC), **FMT_LIM.2/BAC** (BAC): in Personalisation stage only limited test functionality is available. CRC on the personalized data groups can be retrieved during personalization phase only.
- Side channel protection, **FPT_EMS.1** (EAC), **FPT_EMS.1** (SAC), **FPT_EMS.1** (BAC): The TOE uses the platform service “SF_Physical” which relies on its side on the hardware to reduce the side channel leakage.
- Prevention of malfunction, **FPT_FLS.1** (SAC), **FPT_FLS.1/BAC** (BAC): The TOE uses the platform service “SF_Physical” which relies on its side on the hardware to detect
- Self-tests, **FPT_TST.1**: During startup of the Java Card OS the UMSLC (User Mode Security Life Control) selftest offered by the hardware platform is performed.
- Physical protection, **FPT_PHP.3**: The TOE uses the platform services “SF_Physical”.

References

[AIS31] Functionality classes and evaluation methodology for physical random number generators. AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik.

[CCPart1] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model

[CCPart2] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components

[CCPart3] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 3: Security assurance components

[CCPart5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022, Revision 1

[CCErrata] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), V1.1, 2024-07-22

[CCTrans] CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022, 2023-04-20

[CEM2022] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, November 2022, CEM:2022, Revision 1

[CompositeEvaluation] Composite product evaluation for Smart Cards and similar devices, April 2012, Version 1.2, CCDB-2012-04-001

[EU-eMRTD] EU – eMRTD Specification. ANNEX to the Commission Implementing Decision laying down the technical specifications regarding the standards for security features and biometrics in passports and travel documents issued by Member States and repealing Decisions C(2006) 2909 and C(2008) 8657

[TR_ECC] Federal Office for Information Security (BSI) TR-03111 Elliptic Curve Cryptography Version 2.0, 2012-06-28

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

[ICAO_9303_01] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Eighth Edition, 2021, International Civil Aviation Organization

[ICAO_9303_10] International Civil Aviation Organization, DOC 9303 Machine Readable Travel Documents Eighth Edition – 2021, 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 Eighth Edition – 2021 Part 11: Security Mechanisms for MRTD's

[ISO9797-1] ISO/IEC International Standard 9797-1:2011-(E), Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechnanisms using a block cipher, Second Edition 2011-03-01

[ISO14443-3] ISO/IEC International Standard 14443-3 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision, Fourth edition 2018-07

[ISO14443-4] ISO/IEC International Standard 14443-4 Cards and security devices for personal identification Contactless proximity objects, Part 4: Transmission protocol, Fourth edition 2018-07

[ISO7816-3] ISO/IEC 7816-3:2006(E): International Standard ISO 7816-3: Identification cards - Integrated circuit cards, Part 3: Electronic signals and transmission protocols, Third edition 2006-11-01

[ISO7816-4] ISO/IEC JTC1/SC17 International Standard 7816-4: Identification Cards - Integrated circuit cards, Part 4: Organization, security and commands for interchange, Third edition 2013-04-15

[ISO7816-8] International Standard 7816-8: Identification Cards - Integrated circuit cards, Part 8: Commands and Mechanisms for Security Operations, Fifth edition 2021-08

[ISO7816-9] International Standard 7816-9: Identification Cards - Integrated circuit cards, Part 9: Commands for card management, Third edition 2017-12

[ISO9796-2] ISO/IEC International Standard ISO9796-2 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[NIST_Hash] FIPS PUB 180-4, Federal Information Processing Standards Publication Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, March 2012

[NIST_DES] FIPS PUB 46-3: Data Encryption Standard (DES), Reaffirmed, 1999 October 25

[GPv2_3_1] Global Platform Card Specification v2.3.1, March 2018

[UserGuideAdmin] Infineon Applet Collection - eMRTD V2.0 (SLJ38Gxymm1ap) Administration Guide, Revision 1.1, 2025-01-28

[UserGuideDatasheet] Infineon Applet Collection - eMRTD V2.0 (SLJ38Gxymm1ap) Extended Datasheet, Revision 1.3, 2025-03-19

[ST_HW_Platform] IC Security Target BSI-DSZ-CC-1169-V4-2024

[ST_JC_Platform] SECORA™ ID v2.01 (SLJ38Gxymm1ap) Security Target - NSCIB-CC-2400062-01

[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_2] Federal Office for Information Security (BSI) Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.21, 21 December 2016

[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

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

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

[PP_SAC] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22.7.2014, BSI-CC-PP-0068-V2-2011-MA-01, Bundesamt für Sicherheit in der Informationstechnik.

[PP_EAC] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 5.12.2012, BSI-CC-PP-0056-V2-2012, Bundesamt für Sicherheit in der Informationstechnik.

[PP_0084] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, BSI-CC-PP-0084-2014

[FIPS_197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. Department of Commerce/National Institute of Standards and Technology, November 26, 2001

[SOC] SoC for ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0, Revision 0.3, 2025-01-24

Revision history

Reference	Description
Revision 1.0, 2025-03-21	
All	Version for certification

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2025-03-21

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
csscustomerservice@infineon.com

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”).

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.