MASKTECH

SECURITY TARGET

COMMON CRITERIA DOCUMENTS | Version 1.2

MaskTech ePP Applet on Secora™ ID S v1.1

Java Card applet providing Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE

Certification-ID: NSCIB-CC-299277

Public Version

MaskTech International GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Contents

1 ST Introduction (ASE_INT.1)

1.1 ST Reference

Title	Security Target – MaskTech ePP Applet on Secora™ ID S v1.1
Version	1.2, 2022-09-09
Editors	Thomas Rölz
Compliant to	Common Criteria Protection Profiles [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2]
CC Version	3.1 (Revision 5)
Assurance Level	The assurance level for this ST is EAL5 augmented for EAC/PACE and EAL4 augmented for BAC
Keywords	Javacard, Applet, ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)

1.2 TOE Reference

TOE name	MaskTech ePP Applet on Secora™ ID S v1.1
TOE version	1.0
Applet ID	0x0025
TOE hardware	IFX_CCI_000005 by Infineon Technologies AG
Javacard OS platform	Secora™ ID S v1.1 by Infineon Technologies AG
Javacard OS certification	CC-22-175887

1.3 TOE Identification

It is possible to receive the applet ID of the MaskTech ePP Applet on Secora™ ID S v1.1 by personalizing the Helper applet according to [AGD_ePP] Section “Applet ID” in the Helper chapter. The platform can be identified according to section “Platform Information”[1].

[1] Both queries are possible only in the personalization phase.

1.4 TOE Overview

This security target defines the security objectives and requirements for the MaskTech ePP Applet on Secora™ ID S v1.1 as machine readable travel document (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). While the ICAO specification describes only contactless operation the TOE may also support contact based operation in order to allow for non-ICAO contact based products to be realized, eg. national ID cards or MRTD/SSCD combinations. Both interfaces provide the same functionality and are thus taken as one single product in this ST. The MaskTech ePP Applet on Secora™ ID S v1.1 actually comprises several applets mentioned in 1.5.1 that together with the platform components yield the TOE.

1.4.1 TOE Definition

The Target of Evaluation (TOE) addressed by this Security Target is an electronic travel document representing a contactless or contact-based smart card corresponding to [ICAO_9303] and [BSI_TR-03110]. It provides the following application:

- The travel document containing the related user data (incl. biometric if applicable) as well as data needed for authentication via BAC, PACE, EAC or AA protocols,(incl. BAC/PACE passwords); this application is intended to be used by governmental organisations, amongst other 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.

In the context of this Security Target the MRTD functionality is provided by the MaskTech ePP Applet on Secora™ ID S v1.1 to be used exclusively on the Secora™ ID S v1.1 Java Card Platform Implementation for Infineon on IFX_CCI_000005 (SLJ52GxxyyyzS) which is certified CC EAL6 augmented (CC-22-175887). The Java Card platform is provided in the FLASH of a smart card based on the IFX_CCI_000005 chip of Infineon Technologies AG which is itself also certified CC EAL6 augmented. The applet provides standard BAC authentication as well as EAC/PACE protocol with advanced security methods Password Authenticated Connection Establishment, Extended Access Control, Chip Authentication Version 1 described in [BSI_TR-03110], and Active Authentication of [ICAO_9303]. The assurance level for the TOE in BAC mode is CC EAL4 augmented with ALC_DVS.2. The assurance level for the TOE in EAC/PACE mode is CC EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

1.4.1.1 BAC Mode

The Target of Evaluation (TOE) is an electronic travel document (MRTD)[2] representing a contactless/contact-based smart card programmed according to the Logical Data Structure (LDS) and providing Basic Access Control according to [ICAO_9303].

1.4.1.2 EAC/PACE Mode

The Target of Evaluation (TOE) is an electronic travel document (MRTD) representing a contactless/contact-based smart card programmed according to ICAO Technical Report "Supplemental Access Control" [ICAO_SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in [ICAO_9303]) and additionally providing the Extended Access Control according to [ICAO_9303] and [BSI_TR-03110], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), [CC_PP-0068-V2]. Additionally, Active Authentication according to [ICAO_9303] is provided.

1.4.2 TOE Operational Usage

A State or Organization issues travel documents to be used by the holder for international travel. The traveler presents a travel document to the inspection system to prove his or her identity. The travel document in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ) and (iii) data elements on the travel document's chip according to LDS [ICAO_9303] for contactless or contact based machine reading. The authentication of the traveler is based on (i) the possession of a valid travel document personalized 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 organization ensures the authenticity of the data of genuine travel documents. The receiving state trusts a genuine travel document of an issuing State or Organization.

1.4.3 TOE major security features

1.4.3.1 Security features of the platform

The TOE relies on the following security features of the Java Card platform Secora™ ID S v1.1.

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)

[2] The TOE's MRTD functionality claimed by this Security Target is realized by configuration of the MaskTech ePP Applet on Secora™ ID S v1.1 as MRTD. Additionally, the applet can be configured as an ISO-compliant driving license (IDL) which is not in the scope of this certification.

- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to [BSI_AIS31])
- Secure channel SCP03 from [GP_SCP03]
- Content management provided by [GP]
- LDS-API according to [ICAO_9303]
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially hardened against side channel attacks.

1.4.3.2 General security features

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

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

1. the biographical data on the biographical data page of the travel document surface,
2. the printed data in the Machine Readable Zone (MRZ) and
3. the printed portrait.

the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO_9303] as specified by ICAO on the contactless/contact-based integrated circuit. It presents contactless or contact based readable data including (but not limited to) personal data of the travel document holder

1. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
2. the digitized portraits (EF.DG2),
3. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[3],
4. the other data according to LDS (EF.DG5 to EF.DG16) and
5. the Document Security Object (SOD).

The issuing State or Organization implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO_9303]. These security measures can include the binding of the travel document's chip to the travel document.

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

[3]These biometric reference data are optional according to [ICAO_9303]. This ST assumes that the issuing State or Organisation uses this option and protects these data by means of extended access control.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [ICAO_9303] and Password Authenticated Connection Establishment [ICAO_SAC]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism (EAC/PACE) and Basic Access Control (BAC). This security target also addresses the Chip Authentication Version 1 described in [BSI_TR-03110] as an additional alternative to the Active Authentication stated in [ICAO_9303].

1.4.3.3 BAC Mode

The Basic Access Control is a mandatory security feature of the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (Secure Messaging) with this inspection system [ICAO_9303], normative appendix 5.

1.4.3.4 EAC/PACE Mode

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [CC_PP-0068-V2]. Note that [CC_PP-0068-V2] considers high attack potential.

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

1. The travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
2. The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
3. The travel document's chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
4. Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [BSI_TR-03110, ICAO_SAC].

This security target requires the TOE to implement Active Authentication described in [ICAO_9303]. This protocol provides evidence of the travel document's chip authenticity.

This security target requires the TOE to implement the Extended Access Control as defined in[BSI_TR-03110]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1).

The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.5 TOE Description

1.5.1 Component Overview

The TOE is the MaskTech ePP Applet on Secora™ ID S v1.1 installed on the Java Card Secora™ ID S v1.1 which is based on the Smart Card IC IFX_CCI_000005.

The TOE comprises

- the circuitry of the travel document's chip (IFX_CCI_000005),
- the IC Dedicated Software provided by Infineon Technologies AG,
- the IC Embedded Software, the Java Card Platform (Secora™ ID S v1.1) for Infineon Technologies AG on IFX_CCI_000005.
- the ePP Applet provided by MaskTech International GmbH
- the Helper Applet provided by MaskTech International GmbH
- the PACE Applet provided by MaskTech International GmbH
- the TLV-Library provided by MaskTech International GmbH and
- the associated guidance documentation[4] [AGD_ePP]

Figure 1.1 shows the components of the TOE in a layered structure. The blue outline encloses all components being part of the composite TOE covered in this Security Target.

[4]The User Manual (Administration Guide) provides guidance to perform installation/personalization and maintain the targeted security level during Personalization and Operation phase.

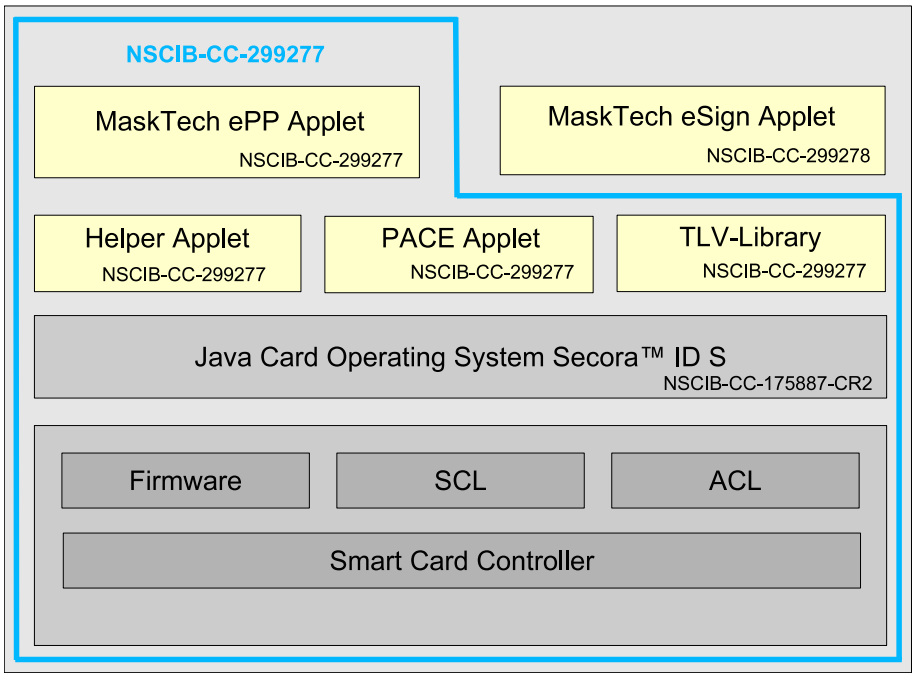

Figure 1.1: Components of the MaskTech ePP Applet on Secora™ ID S v1.1

The bottom layer represents the hardware consisting of

- Smart Card Controller (IFX_CCI_000005)
- Firmware
- Symmetric Crypto Library (SCL)
- Asymmetric Cryptographic Library (ACL) and

The hardware is CC certified and provides protection against fault attacks and side channel attacks. It also provides hardware co-processors supporting cryptographic standards AES, RSA, EC, and 3DES.

The layer above the hardware represents the JavaCard Operating System Secora™ ID S v1.1. It is CC certified as CC-22-175887 and provides security services for

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)
- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to [BSI_AIS31])
- Secure channel SCP03 from [GP_SCP03]
- Content management provided by [GP]
- LDS-API according to [ICAO_9303]
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially hardened against side channel attacks.

The light yellow blocks represent the the applets provided by MaskTech International GmbH that together yield the MaskTech ePP Applet on Secora™ ID S v1.1. Only the components surrounded by the blue outline are part of TOE and responsible for the following tasks:

- MaskTech ePP Applet provides the MRTD functionality (BAC, PACE, EAC, CA, TA, AA).
- MaskTech Helper Applet provides functionality for Secure Messaging as well as buffer handling.
- MaskTech PACE Applet provides functionality for the PACE protocol. It is optional and not used if the MRTD is BAC-only.
- MaskTech TLV-Library provides functionality for TLV-handling during communication with the TOE.

N The MaskTech eSign applet also shown in figure 1.1 is not part of the TOE but may co-exist with MaskTech ePP Applet on Secora™ ID S v1.1 on the same card. It is covered by another certification (NSCIB-CC-299278). Other (third-party) applets are not allowed by the side of MaskTech ePP Applet on Secora™ ID S v1.1 according to [AGD_ePP]

1.5.2 TOE Interfaces

The physical and logical interfaces of the TOE are as follows:

- The physical interface of the TOE is the entire surface of the IC.
- The contact based interface according to [ISO_7816-3].
- The RF interface for contactless communication according to [ISO_14443] Type B.
- The command interface for communication with the TOE provided by the MRTD Application.

1.5.3 Packaging

The applets provided by MaskTech International GmbH are packaged in cap-files to be used on modules according to [SECORA_ST-SLJ52], section '1.4.3 TOE package types'. The cap files can be delivered to the customer in three ways:

- The cap-files are pre-loaded onto the chips by the IC manufacturer Infineon Technologies AG. In this case the cap-files are transferred to Infineon Technologies AG using their proprietary certified delivery procedures.
- The cap-files are loaded onto the chips by MaskTech International GmbH.
- The cap-files are loaded onto the chips by the customer. In this case cap-files are transfered to the customer electronically using the certified delivery procedures of MaskTech International GmbH (encrypted, signed). Cap-file installation is explained in [AGD_ePP], chapter "Applet Installation". The guidance in PDF-format can be downloaded by the customer from the MaskTech web site.

1.5.4 TOE life cycle

The PPs [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] describe the TOE life cycle in terms of four life cycle phases subdivided into 7 steps.

Phase 1 Development

Step 1 Infineon Technologies AG develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

Step 2 Infineon Technologies AG in the role of the software developer [5] uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (Secora™ ID S v1.1 Java Card operating system). MaskTech International GmbH in the role of the software developer develops the ePassport application (MaskTech ePP Applet on Secora™ ID S v1.1) and the guidance documentation associated with this TOE component.

Phase 2 Manufacturing

Step 3 Infineon Technologies AG writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. Infineon Technologies AG adds the parts of the IC Embedded Software (Secora™ ID S v1.1 Java Card operating system) in the non-volatile programmable memory. The IC is securely delivered from Infineon Technologies AG to the travel document manufacturer.

Step 4 (optional) The travel document manufacturer combines the IC with hardware for the contactless/contact-based interface in the travel document unless the travel document consists of the card only.

N In case of contactless TOEs the inlay production including the application of the antenna is NOT part of the TOE and is done after delivery.

Step 5 The travel document manufacturer (i) loads the MaskTech ePP Applet on Secora™ ID S v1.1 into the non-volatile programmable memory if necessary, (ii) creates the ePassport application, and (iii) equips travel document's chips with pre-personalization Data.

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

Note 1: Creation of the application implies applet instantiation.

[5] Note that in this ST the role software developer of the protection profile is subdivided into two separate roles: The operating system is developed by the OS software developer (Java Card, Infineon Technologies AG), and the application by the Java Card applet developer (MRTD, MaskTech International GmbH).

Phase 3 Personalization of the travel document

Step 6 The personalization of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrollment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the personalization of the visual readable data onto the physical part of the travel document, (iv) the writing of the TOE User Data and TSF Data into the logical travel document and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document Security Object.

The signing of the Document security object by the Document signer [ICAO_9303] finalizes the personalization of the genuine travel document for the travel document holder. The personalized travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

N Personalization includes the installation of the applet loaded in phase 2. After the personalization of the product has been done, the Secora™ ID S v1.1 operating system is switched to its proprietary native mode which disables GP and identification commands to avoid tracking as well as loading/installation of 3rd party applets.

Note 2: The role of the *Manufacturer* performing pre-personalization (loading of the ePP package) is taken over by Infineon Technologies AG, MaskTech International GmbH, Linxens (Thailand) Co Ltd. (former SMARTRAC TECHNOLOGY Ltd., see [SC_Linxens]), HID Global Ireland (see [SC_HID]) or HID Global Malaysia (see [SC_HID_MY]).

Phase 4 Operational Use

Step 7 The TOE is used as a travel document's 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.

1.5.5 Non-TOE hardware/software/firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip, the Secora™ ID S v1.1 operating system, and the application (MaskTech ePP Applet on Secora™ ID S v1.1). Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

2 Conformance Claims (ASE_CCL.1)

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 [CC_Part1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 [CC_Part2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 [CC_Part3]

as follows

- Part 2 extended
- Part 3 conformant

The

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

has to be taken into account.

2.2 PP Reference

2.2.1 BAC Mode

For BAC mode this ST claims the strict conformance to the Common Criteria Protection Profile – Machine Readable Travel Document with “ICAO Application”, Basic Access Control, [CC_PP-0055].

2.2.2 EAC/PACE Mode

For EAC/PACE mode this ST claims the strict conformance to the Common Criteria Protection Profile – ’Machine Readable Travel Document with ’ICAO Application’, Extended Access Control with PACE (EAC PP)’, [CC_PP-0056-V2] and to the Common Criteria Protection Profile –

'Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)', [CC_PP-0068-V2].

2.3 PP Additions

Active Authentication based on [ICAO_9303] has been added. This implies the following augmentations:

1. Extension of existing Assumptions for the TOE
   - A.Insp_Sys
   - A.Auth_PKI
2. Addition of new TOE Objectives
   - OT.Active_Auth_Proof
3. Addition of new IT Environment Objectives
   - OE.Active_Auth_Key_Travel_Document
4. Addition of new SFRs for the TOE
   - FCS_COP.1/AA
   - FIA_API.1/AA
   - FMT_MTD.1/AAPK
   - FMT_MTD.1/KEY_READ_AA: Inclusion of the Active Authentication Private Key

The evaluation of the TOE uses the result of the CC evaluation CC-22-175887 of the platform claiming conformance to [CC-PP-2010/03-M01].

2.4 Package Claim

- BAC mode: Package conformant to EAL4 augmented with ALC_DVS.2 defined in [CC_Part3].
- EAC/PACE mode: Package conformant to EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in [CC_Part3].

2.5 Conformance rationale

This ST claims strict conformance to the following protection profiles:

- [CC_PP-0055] (BAC)
- [CC_PP-0056-V2] (EAC) and
- [CC_PP-0068-V2] (PACE)

3 Security Problem Definition (ASE_SPD.1)

3.1 Security Problem Definition from claimed PPs

For this Security Target all assets, subjects and external entities, assumptions, threats, and organisational security policies from section 3 “Security Problem Definition” of [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] are applicable.

3.2 Assumptions refined in this ST

In order to cover Active Authentication from [ICAO_9303] as a means to verify the identity and authenticity of the travel document’s chip as issued by the identified issuing State or Organisation this Security Target refines the following Assumption from [CC_PP-0056-V2].

A.Insp_Sys (Inspection Systems for global interoperability) The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO_SAC] and/or BAC [CC_PP-0055]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. **Optionally all the Inspection Systems can implement Active Authentication.**

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [CC_PP-0068-V2] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

A.Auth_PKI (PKI for Inspection Systems) The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of

the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip. **Optionally the issuing and receiving States or Organisations establish a public key infrastructure to also implement Active Authentication.**

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [CC_PP-0068-V2] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

4 Security Objectives (ASE_OBJ.2)

4.1 Security Objectives from claimed PPs

For this Security Target all Security Objectives for the TOE and for the Operational Environment from section 4 “Security Objectives” of [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] are applicable.

4.2 Security Objectives defined/refined in this ST

In order to cover Active Authentication from [ICAO_9303] as a means to verify the identity and authenticity of the travel document’s chip as issued by the identified issuing State or Organisation this Security Target adds/refines the following security objectives.

OT.Active_Auth_Proof (Proof of 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 Organization by means of the Active Authentication as defined in [ICAO_9303]. The authenticity proof provided by travel document’s chip shall be protected against attacks with high attack potential.

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

OE.Exam_Travel_Document (Examination of the physical part of the travel document) The inspection system of the receiving State or Organization must examine the travel document presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [ICAO_SAC] and/or the Basic Access Control [ICAO_9303]. Extended Inspection Systems perform addition-

ally to these points **the Active Authentication Protocol as defined in [ICAO_9303] and/or** the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

4.3 Security Objective Rationale

The Security Objectives from section 4 "Security Objectives" of [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] are consistent. The Security Objectives **OT.Active_Auth_Proof**, **OE.Active_Auth_Key_Travel_Document** additionally defined in this ST and **OE.Exam_Travel_Document** refined in this ST counter the threat T.Counterfeit from [CC_PP-0056-V2] in the Active Authentication context.

5 Extended Components Definition (ASE_ECD.1)

This Security Target uses the components defined in chapter 5 of [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2]. There are no extended components additionally defined in this ST.

6 Security Requirements (ASE_REQ.2)

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 of the CC [CC_Part1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and that added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined text. Selections filled in by the ST author are denoted as double-underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP author are denoted by showing as underlined text. Assignments filled in by the ST author are denoted as double-underlined text.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal", "MRTD Holder", "Traveller", "Document Signer", "Country Signing Certification Authority", "Attacker" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 8 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CC_Part2]. The operation "load" is synonymous to "import" used in [CC_Part2].

Definition of security attributes:

Security attribute	Values	Meaning
Terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalization Agent	Terminal is authenticated as Personalization Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.
	CVCA	roles defined in the certificate used for authentication (cf. [BSI_TR-03110]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [BSI_TR-03110]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [BSI_TR-03110]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [BSI_TR-03110]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [BSI_TR-03110])
	DG3 (Fingerprint)	Read access to DG3: (cf. [BSI_TR-03110])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [BSI_TR-03110])

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [CC_PP-0068-V2].

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying	The TOE stores the Country Verifying Certification Authority
Certification Authority Public Key (PK_{CVCA})	Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [5] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [ISO_11770-3].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.

Name	Data
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Active Authentication Public Key Pair	The Active Authentication Public Key Pair (SK_{AA}, PK_{AA}) are used for Active Authentication according to [ICAO_9303].
Active Authentication Public Key (PK_{AA})	The Active Authentication Public Key (PK_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key (SK_{AA})	The Active Authentication Private Key (SK_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

6.1 Security Functional Requirements for the TOE

Because this ST claims conformance to the protection profiles [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] the Security Functional Requirents of those PPs are covered in the following sections.

6.1.1 SFRs from [CC_PP-0055] (BAC) and [CC_PP-0068-V2] (PACE)

Some SFRs are part of [CC_PP-0055] as well as [CC_PP-0068-V2] and furthermore, functionally equivalent. Consequently, they can be combined to be handled only once.

6.1.1.1 Class Cryptographic Support (FCS)

FCS_CKM.4	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]: fulfilled by FCS_CKM.1/DH_PACE (PACE) and FCS_CKM.1 (BAC)
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with random values that meets the following: none.

N According to application note 19 from [CC_PP-0055] the SM keys (ENC/MAC) must be destroyed. Application note 28 from [CC_PP-0068-V2] extends this to PACE session keys. As there is no contradiction this SFR need not be separated for BAC and EAC.

FCS_RND.1	Quality metric for random numbers
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet the Class PTG.3 quality metric according to [BSI_AIS31].

N Both, application note 24 from [CC_PP-0055] as well as application note 31 from [CC_PP-0068-V2] are applicable here. The random numbers generated according to FCS_RND shall be used for BAC and PACE as defined in FIA_UAU.4 and FIA_UAU.4/PACE (including 3DES authentication). As there is no contradiction this SFR need not be separated for BAC and EAC.

6.1.1.2 Class FMT Security Management

FMT_MTD.1/INI_ENA	Management of TSF data – Writing Initialization and Pre-personalization Data
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 (PACE) and FMT_SMF.1/BAC (BAC) FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE (PACE) and FMT_SMR.1 (BAC)
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

N Application note 42 from [CC_PP-0055] defines “Pre-Personalization Data” in a way that also applies to FMT_MTD.1/INI_ENA from [CC_PP-0068-V2]. As there is no contradiction this SFR need not be separated for BAC and EAC.

6.1.1.3 Class FPT Protection of the Security Functions

FPT_TST.1	TSF testing
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

N The meaning of application note 46 from [CC_PP-0055] is equivalent to the meaning of application note 52 from [CC_PP-0068-V2]. As there is no contradiction this SFR need not be separated for BAC and EAC.

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.

N Application note 47 from [CC_PP-0055] and application note 53 from [CC_PP-0068-V2] are identical. As there is no contradiction this SFR need not be separated for BAC and EAC.

6.1.2 SFRs from [CC_PP-0055] (BAC)

Some of the SFRs in [CC_PP-0055] are also part of [CC_PP-0056-V2] and/or [CC_PP-0068-V2]. Because they are functionally different from their counterparts they are distinguished by adding the iteration “/BAC” to their name.

6.1.2.1 Class FAU Security Audit

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.

Note 3: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 *Manufacturing*. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or pre-personalization data as TSF data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2.2 Class Cryptographic Support (FCS)

FCS_CKM.1	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [ICAO_9303_1], normative appendix 5.

Note 4: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [ICAO_9303], normative appendix 5, A5.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

FCS_COP.1/SHA	Cryptographic operation – Hash for Key Derivation by MRTD
PP reference:	[CC_PP-0055]
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: [FIPS_180-4].

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] FCS_CKM.4 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 size 112 bit that meet the following: [NIST_SP800-67] and [ICAO_9303_1]; normative appendix 5, A5.3.

Note 5: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH	**Cryptographic operation – Authentication**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication - encryption and decryption in accordance with a specified cryptographic algorithm AES **in CBC mode** and cryptographic key sizes 128 bit that meet the following: [FIPS_197].

Note 6: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC	Cryptographic operation – Retail MAC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
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).

Note 7: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

6.1.2.3 Class FIA Identification and Authentication

Note 8: Table 6.1 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO_9303], Annex E, and [BSI_TR-03110]
Basic Access Control Authentication Mechanism	FIA_AFL.1, FIA_UAU.4, FIA_UAU.6	Triple-DES, 112 bit keys; Retail-MAC, 112 bit keys
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	AES, 128 bit keys

Table 6.1: Overview on authentication SFR

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 “Personalization 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.

Note 9: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 “Manufacturing”. The audit records can be written only in the Phase 2 “Manufacturing of the TOE”. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer creates the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the MRTD”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

Note 10: In the “Operational Use” phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD’s chip use a randomly chosen identifier for the communication channel to allow the terminal to communicate with more then one RFID. This identifier will not violate the OT.Identification.

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow 1. to read the Initialization Data in Phase 2 “Manufacturing” 2. to read the random identifier in Phase 3 “Personalization of the MRTD” 3. to read the random identifier in Phase 4 “Operational Use” 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.

Note 11: The Basic Inspection System and the Personalization Agent authenticate themselves.

FIA_UAU.4	**Single-use authentication mechanisms – Single-use authentication of the Terminal by the TOE**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism 2. Authentication Mechanism based on Triple-DES **and** AES

Note 12: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

Note 13: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [ICAO_9303]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

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. Secure Channel Protocol SCP03 specified in [GP_SCP03] with *Personalization Agent* Keys to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. The TOE accepts the authentication attempt as *Personalization Agent* by one of the following mechanisms (a) the Secure Channel Protocol SCP03 of Global Platform with *Personalization Agent* Keys. 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

Note 14: The Basic Access Control Mechanism includes the Secure Messaging for all commands exchanged after successful authentication of the inspection system. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

N As with FIA_UAU.5/PACE this SFR allows for authentication of the personalization agent via SCP03 specified in [GP_SCP03] of Global Platform ([GP]) during personalization.

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.

Note 15: The Basic Access Control Mechanism specified in [ICAO_9303] includes the Secure Messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by Secure Messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Note 16: Note that in case the TOE should also fulfill [CC_PP-0056] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.

FIA_AFL.1	Authentication failure handling
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when an administrator configurable number of unsuccessful authentication attempt occurs related to BAC authentication.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall wait for an administrator configurable time between the reception of the authentication command and its processing.

Note 17: The TSF shall detect when an administrator configurable positive integer within range of acceptable values 1 to 10 consecutive unsuccessful authentication attempts occur related to BAC authentication protocol. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall wait for an administrator configurable time between the receiving the terminal challenge eIFD and sending the TSF response eICC during the BAC authentication attempts. The terminal challenge eIFD and the TSF response eICC are described in [BSI_TR-03110], Appendix C. The refinement by inclusion of the word “consecutive” allows the TSF to return to normal operation of the BAC authentication

protocol (without time out) after successful run of the BAC authentication protocol. The unsuccessful authentication attempt shall be stored non-volatile in the TOE thus the “consecutive unsuccessful authentication attempts” are count independent on power-on sessions but reset to zero after successful authentication only.

N Delay behaviour in case of unsuccessful authentication attempts can be configured with a granularity of 1/10 of a second during peronalisation (max. 12.7 seconds).

6.1.2.4 Class FDP User Data Protection

FDP_ACC.1	**Subset 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.

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the Basic Access Control SFP to objects based on the following: 1. Subjects: (a) Personalization 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 Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules: 1. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD 2. Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD 3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Note 18: The inspection system needs special authentication and authorization for read access to DG3 and DG4 defined in [CC_PP-0056].

Note 19: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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 objects in a manner protected from unauthorized disclosure.

FDP_UIT.1	**Data exchange integrity – MRTD**
Hierarchical to:	No other components.

Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the Basic Access Control SFP 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

6.1.2.5 Class FMT Security Management

Note 20: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

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 security management functions: 1. Initialization 2. Pre-personalization 3. Personalization

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	The TSF shall maintain the roles: 1. Manufacturer 2. Personalization Agent 3. Basic Inspection System
FMT_SMR.1.2	The TSF shall be able to associate users with roles

Note 21: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

FMT_LIM.1/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 be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery do not allow 1. User Data to be disclosed or manipulated 2. TSF data to be disclosed or manipulated 3. Software to be reconstructed 4. Substantial information about construction of TSF to be gathered which may enable other attacks

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 their capabilities 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 disclosed or manipulated 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

Note 22: The formulation of "Deploying Test Features ..." in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

FMT_MTD.1/INI_DIS/BAC	**Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: 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 Initialization Data to the Personalization Agent

Note 23: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE restricts the ability to write the Initialization Data and the Prepersonalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer writes the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access will be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_WRITE	**Management of TSF data – Key Write**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent

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 Personalization Agent Keys to none

Note 24: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

6.1.2.6 Class FPT Protection of Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

FPT_EMSEC.1	TOE Emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to Personalization Agent Key(s) and Document Basic Access Keys.
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and Document Basic Access Keys.

Note 25: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface but may have also (not used by the terminal but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

FPT_FLS.1/BAC	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1/BAC	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to out-of-range operating conditions where therefore a malfunction could occur 2. failure detected by TSF according to FPT_TST.1

6.1.3 SFRs from [CC_PP-0056-V2] (EAC)

The following section covers the SFRs from [CC_PP-0056-V2] (EAC) as well as those SFRs from [CC_PP-0068-V2] (PACE/SAC) that are extended in the EAC-PP (see respective application notes below the SFRs). Furthermore, the additional SFRs necessary to cover the Active Authentication functionality from [ICAO_9303] are listed here.

6.1.3.1 Class Cryptographic Support (FCS)

FCS_COP.1/AA	Cryptographic operation – Signature creation by travel document – 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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AA	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA with SHA-1/SHA224/SHA256/SHA384/SHA512 and cryptographic key sizes 1024/1536/2048 bits that meet the following: [ISO_9796-2] **and** in accordance with a specified cryptographic algorithm ECDSA with SHA-1/SHA224/SHA256/SHA384/SHA512 and cryptographic key sizes 192/224/256/384/512(BP)/521(NIST) bits that meet the following: [BSI_TR-03110-1] .

FCS_CKM.1/CA	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH and specified cryptographic key sizes 112 bits (TDES) and 128/192/256 bits (AES) that meet the following: ECDH protocol compliant to [BSI_TR-03111]

Note 26: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [BSI_TR-03110].

Note 27: The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [CC_PP-0068-V2] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption / Decryption
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_ENC	The TSF shall perform secure messaging - encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and cryptographic key sizes 128/192/256 bit **and** 3DES in CBC mode and cryptographic key sizes 112 bit that meet the following: compliant to [BSI_TR-03110-1].

Note 28: This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA.

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and encryption compliant to [NIST_SP800-38A].

FCS_COP.1/CA_MAC	Cryptographic operation – MAC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and cryptographic key sizes 128/192/256 bit **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: compliant to [ICAO_SAC].

Note 29: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalization Agent by means of the authentication mechanism.

N For personalization of the TOE the Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]) is used with AES 256 bits key length and CMAC compliant to [NIST_SP800-38A].

FCS_COP.1/SIG_VER	**Cryptographic operation – Signature verification by travel document**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-1/SHA-224/SHA-256/SHA-384/SHA-512 and cryptographic key sizes 192/224/256/384/512 bits that meet the following: compliant to [BSI_TR-03110-1].

6.1.3.2 Class FIA Identification and Authentication

Table 6.2 provides an overview of the authentication mechanisms used.

Name	**SFR for the TOE**
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication (specified in addition to [CC_PP-0056-V2])	FIA_API.1/AA

Table 6.2: Overview on authentication SFR

Note the Chip Authentication Protocol Version 1 as defined in this protection profile includes

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

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 [BSI_TR-03110-1] 5. to carry out the Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1] 6. to carry out the Active Authentication Mechanism according to [ICAO_9303] 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.

Note 30: The SFR FIA_UID.1/PACE covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

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 v.1 according to [BSI_TR-03110-1] 6. to carry out the Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1] 7. to carry out the Active Authentication Mechanism according to [ICAO_9303] 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.

Note 31: The SFR FIA_UAU.1/PACE in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

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 to [ICAO_SAC], 2. Authentication Mechanism based on Triple-DES **or** AES, 3. Terminal Authentication Protocol v.1 according to [BSI_TR-03110-1].

Note 32: The SFR FIA_UAU.4.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [CC_PP-0068-V2].

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], 3. Secure messaging in MAC-ENC mode according to [ICAO_SAC], 4. Symmetric Authentication Mechanism based on Secure Channel Protocol SCP03 specified in [GP_SCP03] with *Personalization Agent* Keys, 5. Terminal Authentication Protocol v.1 according to [BSI_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 Personalization Agent by the Secure Channel Protocol SCP03 of Global Platform with *Personalization Agent* Keys. 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1. 4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol 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. 5. none

Note 33: The SFR FIA_UAU.5.1/PACE covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 2), 3), 4)and 5). These extensions do not conflict with the strict conformance to PACE PP.

N Item 2 of FIA_UAU.5.2/PACE above defines the authentication of the personalization agent during personalization by means of Secure Channel Protocol SCP03 specified in [GP_SCP03] of Global Platform ([GP]).

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.

Note 34: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO_9303] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

FIA_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 [BSI_TR-03110-1] to prove the identity of the TOE.

Note 35: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [BSI_TR-03110]. The TOE and the terminal generate a shared secret using the Elliptic Curve Diffie-Hellman Protocol (EC-DH only) and two session keys for secure messaging in ENC_MAC mode according to [ICAO_9303]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended [CC_Part2]).

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 an Active Authentication Mechanism according to [ICAO_9303] to prove the identity of the TOE.

6.1.3.3 Class FDP User Data Protection

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

Note 36: The SFR FIA_ACC.1.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to PACE PP.

FDP_ACF.1/TRM	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/TRM	The TSF shall enforce the Access Control SFP to objects based on the following: 1. Subjects: (a) Terminal (b) BIS-PACE (c) Extended Inspection System 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, (d) all TOE intrinsic secret cryptographic keys stored in the travel document. 3. Security attributes: (a) PACE Authentication, (b) Terminal Authentication v.1, (c) Authorization 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/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 DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM. 4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) 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.

Note 37: The SFR FDP_ACF.1.1/TRM covers the definition in PACE PP [CC_PP-0068-V2] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM cover the definition in PACE PP [CC_PP-0068-V2]. The SFR FDP_ACF.1.4/TRM covers the definition in PACE PP [CC_PP-0068-V2] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to PACE PP.

Note 38: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [BSI_TR-03110-1]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Note 39: FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the user data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.1.3.4 Class FMT Security Management

Note 40: The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

FMT_SMR.1/PACE	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 TSF shall maintain the roles: 1. Manufacturer, 2. Personalization Agent, 3. Terminal, 4. PACE authenticated BIS-PACE, 5. Country Verifying Certification Authority, 6. Document Verifier, 7. Domestic Extended Inspection System, 8. Foreign Extended Inspection System.
FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.

Note 41: The SFR FMT_SMR.1.1/PACE in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

Note 42: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User data to be manipulated and disclosed, 2. TSF data to be 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.

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.

Dependencies:	FMT_LIM.1 Limited capabilities
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: 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 and 5. sensitive user data (EF.DG3 and EF.DG4) to be disclosed.

Note 43: The following SFRs are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

FMT_MTD.1/CVCA_INI	**Management of TSF data – Initialization of CVCA Certificate and Current Date**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
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 Verifier Certification Authority Certificate, 3. Initial Current Date, 4. none. to the Personalization Agent

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

Note 44: The authorized roles are identified in their certificate (cf. [BSI_TR-03110]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [BSI_TR-03110]).

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: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to load the Chip Authentication Private Key to the Personalization Agent

FMT_MTD.1/AAPK	**Management of TSF data – Active Authentication Private Key – AA**
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/ AAPK	The TSF shall restrict the ability to load the Active Authentication Private Key to the Personalization Agent

FMT_MTD.1/CVCA_UPD	**Management of TSF data – Country Verifier Certification Authority**
Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
FMT_MTD.1.1/CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifying Certification Authority Public Key, 2. Country Verifier Certification Authority Certificate, to Country Verifier Certification Authority

Note 45: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [BSI_TR-03110]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [BSI_TR-03110]).

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. Chip Authentication Private Key, 3. Personalization Agent Keys. to none.

Note 46: The SFR FMT_MTD.1/KEY_READ in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

FMT_MTD.1/ KEY_READ_AA	Management of TSF data – Key Read – AA
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_AA	The TSF shall restrict the ability to read the Active Authentication Private Key to none

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.

Note 47: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.3.5 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for the User Data and TSF-data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of the TOE security functionality.

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit information about IC power consumption and command execution time in excess of non-useful information enabling access to 1. Chip Authentication Session Keys, 2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. Manufacturer Authentication Key, 5. Administration keys, 6. Personalization Agent Keys, 7. Chip Authentication Private Key, 8. Active Authentication Private Keys,

FPT_EMS.1.2	The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to 1. Chip Authentication Session Keys, 2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. Manufacturer Authentication Key, 5. Administration keys, 6. Personalization Agent Keys, 7. Chip Authentication Private Key, 8. Active Authentication Private Keys,

Note 48: The SFR FPT_EMS.1.1 covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in EAC PP covers the definition in PACE PP [CC_PP-0068-V2] and extends it by EAC aspects 4) and 5). Active Authentication is taken into account in aspect 9 of FPT_EMS.1.1 and FPT_EMS.1.2. These extensions do not conflict with the strict conformance to PACE PP.

6.1.4 SFRs from [CC_PP-0068-V2] (PACE)

6.1.4.1 Class Cryptographic Support (FCS)

FCS_CKM.1/DH_PACE	Cryptographic key generation – Diffie-Hellman for PACE session keys
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.2/DH. Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_CKM.1.1/ DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [BSI_TR-03111] and specified cryptographic key sizes 192/224/256/384/512(BP) bits (ECDH), 112 bits (TDES) and 128/192/256 bits (AES) that meet the following: [ICAO_SAC].

Note 49: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO_SAC]. The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [ICAO_SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Note 50: FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO_SAC].

FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption / Decryption AES/3DES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/PACE_ENC	The TSF shall perform Secure Messaging - encryption and decryption in accordance with the cryptographic algorithm AES in CBC mode and cryptographic key sizes 128, 192 and 256 bits **and** 3DES in CBC mode and cryptographic key sizes 112 bits that meet the following: compliant to [ICAO_SAC].

Note 51: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}).

FCS_COP.1/PACE_MAC	Cryptographic operation – MAC
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4
FCS_COP.1.1/PACE_MAC	The TSF shall perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC and cryptographic key sizes 128/192/256 bit **and** Retail-MAC and cryptographic key sizes 112 bit that meet the following: compliant to [ICAO_SAC].

Note 52: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}).

6.1.4.2 Class FIA Identification and Authentication

The following SFRs of class FIA from [CC_PP-0068-V2]

- FIA_UID.1/PACE
- FIA_UAU.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE

are covered and extended in [CC_PP-0056-V2]. Please refer to section 6.1.3.2.

FIA_AFL.1/PACE	Authentication failure handling – PACE authentication using non-blocking authorization data
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when an administrator configurable number of unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password for PACE.
FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall wait for an administrator configurable time between the reception of the authentication command and its processing.

N Delay behaviour in case of unsuccessful authentication attempts can be configured with a minimum granularity of 1/10 of a second during peronalisation (max. 12.7 seconds).

FIA_UAU.6/PACE	Re-authenticating – 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.

6.1.4.3 Class FDP User Data Protection

The SFRs FDP_ACC.1/TRM and FDP_ACF.1/TRM of class FDP from [CC_PP-0068-V2] are covered and extended in [CC_PP-0056-V2]. Please refer to section 6.1.3.3.

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 DH shared secret K)[1] 3. none

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 unauthorized disclosure.

[1] according to [ICAO_SAC]

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.

6.1.4.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

6.1.4.5 Class FAU Security Audit

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the Manufacturer with the capability to store the Initialization and Pre-personalization Data in the audit records.

Note 53: The *Manufacturer* role is the default user identity assumed by the TOE in the life cycle phase '*Manufacturing*'. The IC *Manufacturer* and the travel document *Manufacturer* in the *Manufacturer* role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see

FMT_ MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.4.6 Class FMT Security Management

The following SFRs of class FMT from [CC_PP-0068-V2]

- FMT_SMR.1/PACE
- FMT_LIM.1
- FMT_LIM.2
- FMT_MTD.1/KEY_READ

are covered and extended in [CC_PP-0056-V2]. Please refer to section 6.1.3.4.

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

FMT_MTD.1/INI_DIS	**Management of TSF data – Reading and Using Initialization and Pre-personalization 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 Initialization Data and the Pre-personalization Data to the Personalization Agent

FMT_MTD.1/PA	**Management of TSF data – Personalization 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 to the Document Security Object (SO_D) to the Personalization Agent

6.1.4.7 Class FPT Protection of the Security Functions

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

The SFR FPT_EMS.1 from [CC_PP-0068-V2] is covered and extended in [CC_PP-0056-V2]. Please refer to section 6.1.3.5.

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

6.2 Security Assurance Requirements for the TOE

For BAC mode of the TOE this Security Target claims EAL4 augmented with ALC_DVS.2 (Sufficiency of security measures). Consequently, section 6.2 'Security Assurance Requirements for the TOE' from [CC_PP-0055] is applicable and exceeded here.

For EAC/PACE mode of the TOE this Security Target claims EAL5 augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis). Consequently, sections 6.2 'Security Assurance Requirements for the TOE' from [CC_PP-0056-V2] and [CC_PP-0068-V2] are applicable and exceeded here.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

Because this Security Target claims [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] their respective sections 6.3.1 'Security Functional Requirements Rationale' are applicable here.

The SFRs additionally defined in this ST cover Active Authentication from [ICAO_9303]:

- FCS_COP.1/AA
- FIA_API.1/AA
- FMT_MTD.1/AAPK
- FMT_MTD.1/KEY_READ_AA

These SFRs were invented to fulfill the following additional objective:

- OT.Active_Auth_Proof

6.3.2 Dependency Rationale

Because this Security Target claims [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] their respective sections 6.3.2 'Rationale for SFR's Dependencies' are applicable here. Table 6.3 shows the dependencies of the additional SFRs of the TOE.

SFR	Dependencies	Dependency Support
FCS_COP.1/AA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation],	justification 1 for non-satisfied dependencies
	FCS_CKM.4 Cryptogr. key destruction	justification 1 for non-satisfied dependencies
FIA_API.1/AA	No dependencies	N/A
FMT_MTD.1/AAPK	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/ KEY_READ_AA	FMT_SMF.1 Specification of management functions,	Fulfilled by FMT_SMF.1
	FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE

Table 6.3: Dependencies of the additional SFRs of the TOE

Justification for non-satisfied dependencies between the SFR for TOE:

No. 1 The SFR FCS_COP.1/AA uses the asymmetric Authentication Key permanently stored during the Personalization process (cf. FMT_MTD.1/INI_ENA) by the Personalization Agent. Thus there is neither the necessity to generate or import a key during the addressed TOE life cycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

6.3.3 Security Assurance Requirements Rationale

6.3.3.1 Security Assurance Requirements Rationale (BAC)

The assurance level EAL4 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

The component ALC_DVS.2 has no dependencies.

All dependencies are met or exceeded in the EAL4 assurance package.

6.3.3.2 Security Assurance Requirements Rationale (EAC/PACE)

The selection of assurance components is based on the underlying PP [CC_PP-0056-V2]. This Security Target uses the same augmentations as the PP, but chooses a higher assurance level. EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 is applicable in those circumstances where developers or users require a very high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs. Additionally, the requirement of the PP [CC_PP-0056-V2] to choose at least EAL4 is fulfilled.

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

The selection of the component ATE_DPT.2 as augmentation from the PP is made obsolete by the selection of EAL5 because the component ATE_DPT.3 as part of EAL5 already exceeds ATE_DPT.2.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfill the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The rationales for the internal consistency of the SFRs from [CC_PP-0055], [CC_PP-0056-V2], and [CC_PP-0068-V2] section 6.3.4 'Security Requirements – Internal Consistency' are applicable here. Furthermore, the rationales for internal consistency between functional and assurance requirements from those PPs are also applicable.

The analysis of the TOE's security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 6.3.2 'Dependency Rationale for the security functional requirements' shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. This is also true for the augmentations specified in section 2.3. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behavior of these 'shared' items.

The assurance classes EAL4 and EAL5 are established sets of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components regarding BAC and EAC/PACE in section 6.3.3 'Security Assurance Requirements Rationale' shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 'Rationale for SFR's Dependencies' and 6.3.3 'Security Assurance Requirements Rationale'. Furthermore, as also discussed in section 6.3.3 'Security Assurance Requirements Rationale', the chosen assurance components are adequate for

the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specification (ASE_TSS.1)

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

7.1 TOE Security Functions

7.1.1 F.Access_Control

F.Access_Control regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. Access Control in the Manufacturing phase (phase 2) while the applet is still absent can only be done by the Manufacturer or on behalf of him based on Global Platform (see SF.CM of the platform). Access Control in the Personalization phase (phase 3) can only be done by the Personalization Agent identified with the respective authentication key (see SF.CM of the platform).

F.Access_Control consists of the following elements:

FIA_UID.1 (BAC), FIA_UID.1/PACE (EAC/PACE) Timing of authentication

- Requires each user to be successfully identified before allowing any other TSF-mediated actions.

FIA_UAU.1 (BAC), FIA_UAU.1/PACE (EAC/PACE) Timing of authentication

- Requires each user to be successfully identified before allowing any other TSF-mediated actions.

FIA_UAU.4 (BAC), FIA_UAU.4/PACE (EAC/PACE) Single-use authentication of the Terminals by the TOE

- Prevent reuse of authentication data related to the BAC, PACE, Terminal Authentication and Active Authentication.

FIA_UAU.5 (BAC), FIA_UAU.5/PACE (EAC/PACE) Multiple authentication mechanisms

- Authentication via BAC, Symmetric Authentication, PACE, Passive Authentication, and Terminal Authentication.
- In the Personalization phase Secure Channel Protocol SCP03 of Global Platform with Personalization Agent keys.

FIA_UAU.6 Re-authenticating of Terminal by the TOE

- Re-authenticate the user after successful run of the BAC Protocol.

FIA_UAU.6/PACE (EAC/PACE) Re-authenticating of Terminal by the TOE

- Re-authenticate the user after successful run of the PACE Protocol.

FIA_UAU.6/EAC (EAC/PACE) Re-authenticating of Terminal by the TOE

- Re-authenticate the user after successful run of the Chip Authentication Protocol.

FIA_AFL.1 (BAC), FIA_AFL.1/PACE (EAC/PACE) Authentication failure handling

- Detect when an administrator configurable number of unsuccessful authentication attempt occurs.
- After the defined number of unsuccessful authentication attempts occured, the TSF waits for an administrator configurable time between the reception of the authentication command and its processing.

FDP_ACC.1 (BAC), FDP_ACC.1/TRM (EAC/PACE) Subset access control – Terminal Access

- Enforce the Access Control SFP on terminals gaining access to the User data and data stored in EF.Sod.

FDP_ACF.1 (BAC), FDP_ACF.1/TRM (EAC/PACE) Security attribute based access control

- Enforce the Access Control SFP on terminals gaining access to the User data and data stored in EF.Sod.

FDP_UCT.1 (BAC), FDP_UCT.1/TRM (EAC/PACE) Basic data exchange confidentiality – MRTD

- Enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

FDP_UIT.1 (BAC), FDP_UIT.1/TRM (EAC/PACE) Data exchange integrity

- 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.
- On receipt of user data determine, whether modification, deletion, insertion and replay has occurred.

FMT_SMR.1 (BAC), FMT_SMR.1/PACE (EAC/PACE) Security roles

- Maintain the roles (1.) Manufacturer , (2.) Personalization Agent , (3) Terminal, (4) PACE authenticated BIS-PACE, (5) Country Verifying Certification Authority, (6) Document Verifier, (7) Domestic Extended Inspection System, and (8) Foreign Extended Inspection System.
- Associate users with roles.

FMT_LIM.1/BAC (BAC), FMT_LIM.1 (EAC/PACE) Limited capabilities

- Limit test features capabilities so that in conjunction with “Limited availability FMT_LIM.2(/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

FMT_LIM.2/BAC (BAC), FMT_LIM.2 (EAC/PACE) Limited availability

- Limit test features availability so that in conjunction with “Limited capabilities FMT_LIM.1(/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (2) TSF data to be disclosed or manipulated, (3) software to be reconstructed, (4) substantial information about con-struction of TSF to be gathered which may enable other attacks, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

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

- Restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent.

FMT_MTD.1/CVCA_UPD (EAC/PACE) Management of TSF data – Country Verifying Certification Authority

- Restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority.

FMT_MTD.1/DATE (EAC/PACE) Management of TSF data – Current date

- Restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System.

FMT_MTD.1/CAPK (EAC/PACE) Management of TSF data – Chip Authentication Private Key

- Restrict the ability to load the Chip Authentication Private Key to the Personalization Agent.

FMT_MTD.1/KEY_READ/BAC (BAC), FMT_MTD.1/KEY_READ (EAC/PACE) Management of TSF data – Key Read

- Restrict the ability to read the Document Basic Access Keys, PACE passwords, Chip Authentication Private Key, and the Personalization Agent Keys to none.

FMT_MTD.1/KEY_READ_AA (EAC/PACE) Management of TSF data – Key Read – AA

- Restrict the ability to read the Active Authentication Private Key to none.

FMT_MTD.1/KEY_WRITE (BAC) Management of TSF data – Key Write

- Restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

FMT_MTD.1/PA (EAC/PACE) Management of TSF data – Personalization Agent

- Restrict the ability to write the Document Security Object (SOD) to the Personalization Agent.

FTP_ITC.1/PACE (EAC/PACE) Inter-TSF trusted channel after PACE

- Provide a communication channel between the TOE 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.

FMT_MTD.1/INI_ENA (BAC, EAC/PACE) Management of TSF data – Writing Initialization and Pre-personalization Data

- Restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

FMT_MTD.1/INI_DIS/BAC (BAC), FMT_MTD.1/INI_DIS (EAC/PACE) Management of TSF data – Reading and Using Initialization and Pre-personalization Data

- Restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

7.1.2 F.Administration

F.Administration covers the administration (storage) of manufacturing data, pre-personalization data and personalization data. Only the Manufacturer or the Personalization Agent are able to write these data once after authentication via Global Platform. Administration of manufacturing and pre-personalization data in life cycle Phase 2 is based on the Global Platform card manager of the Java Card platform (SF.CM). In the Operational Use phase, only read access is allowed and only after successful authentication.

F.Administration consists of the following elements:

FAU_SAS.1/BAC (BAC), FAU_SAS.1 (EAC/PACE) Audit storage

- Provide the Manufacturer with the capability to store the the Initialization and Pre-personalization Data in the audit records.

FMT_SMF.1/BAC (BAC), FMT_SMF.1 (EAC/PACE) Specification of Management Functions

- Provide the following management functions: (1.) Initialization , (2.) Pre-personalization , (3.) Personalization, (4) Configuration.

FMT_SMR.1 (BAC), FMT_SMR.1/PACE (EAC/PACE) Security roles

- Maintain the roles (1.) Manufacturer , (2.) Personalization Agent , (3) Terminal, (4) PACE authenticated BIS-PACE, (5) Country Verifying Certification Authority, (6) Document Verifier, (7) Domestic Extended Inspection System, and (8) Foreign Extended Inspection System.
- Associate users with roles.

FMT_LIM.1/BAC (BAC), FMT_LIM.1 (EAC/PACE) Limited capabilities

- Limit test features capabilities so that in conjunction with “Limited availability FMT_LIM.2(/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (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, (5) sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

FMT_LIM.2/BAC (BAC), FMT_LIM.2 (EAC/PACE) Limited availability

- Limit test features availability so that in conjunction with “Limited capabilities FMT_LIM.1(/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (2) TSF data to be

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

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

- Restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent.

FMT_MTD.1/CVCA_UPD (EAC/PACE) Management of TSF data – Country Verifying Certification Authority

- Restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority.

FMT_MTD.1/DATE (EAC/PACE) Management of TSF data – Current date

- Restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System.

FMT_MTD.1/CAPK (EAC/PACE) Management of TSF data – Chip Authentication Private Key

- Restrict the ability to load the Chip Authentication Private Key to the Personalization Agent.

FMT_MTD.1/KEY_READ/BAC (BAC), FMT_MTD.1/KEY_READ (EAC/PACE) Management of TSF data – Key Read

- Restrict the ability to read the Document Basic Access Keys, PACE passwords, Chip Authentication Private Key, and the Personalization Agent Keys to none.

FMT_MTD.1/KEY_READ_AA (EAC/PACE) Management of TSF data – Key Read – AA

- Restrict the ability to read the Active Authentication Private Key to none.

FMT_MTD.1/KEY_WRITE (BAC) Management of TSF data – Key Write

- Restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

FMT_MTD.1/PA (EAC/PACE) Management of TSF data – Personalization Agent

- Restrict the ability to write the Document Security Object (SOD) to the Personalization Agent.

FMT_MTD.1/INI_ENA (BAC, EAC/PACE) Management of TSF data – Writing Initialization and Pre-personalization Data

- Restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.

FMT_MTD.1/INI_DIS/BAC (BAC), FMT_MTD.1/INI_DIS (EAC/PACE) Management of TSF data – Reading and Using Initialization and Pre-personalization Data

- Restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

7.1.3 F.Crypto

F.Crypto provides a high level interface to

- DES
- AES
- CMAC
- 3DES/CBC
- DES/Retail MAC
- RSA
- Random number generation

F.Crypto consists of the following elements:

FCS_CKM.1 (BAC), FCS_CKM.1/DH_PACE and FCS_CKM.1/CA (EAC/PACE) Cryptographic key generation

- Generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm, Elliptic Curve Diffie-Hellman-Protocol (ECDH).

FCS_CKM.4 (BAC, EAC/PACE) Cryptographic key destruction – Session keys

- Destroy cryptographic keys in accordance with the cryptographic key destruction method "physically overwriting the keys with random values via the clearKey method of the platform.

FDP_RIP.1 (EAC/PACE) Subset residual information protection

- Make sure that any previous information content of a resource is made unavailable upon the deallocation of the resource.

FCS_COP.1/ENC (BAC), FCS_COP.1/PACE_ENC (EAC/PACE) Cryptographic operation - Encryption / Decryption AES/3DES

- Perform Secure Messaging - encryption and decryption in accordance with the cryptographic algorithm AES in CBC mode and 3DES in CBC mode. For PACE the PACE API of the platform is used.

FCS_COP.1/MAC (BAC), FCS_COP.1/PACE_MAC (EAC/PACE) Cryptographic operation – MAC

- Perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and Retail-MAC. For PACE the PACE API of the platform is used. For Secure Messaging the proprietary Infineon Secure Messaging Accelerator Class is used.

FCS_COP.1/SHA (BAC) Cryptographic operation – Hash for Key Derivation by MRTD

- Perform hashing in accordance with a specified cryptographic algorithm SHA-1.

FCS_COP.1/CA_ENC (EAC/PACE) Cryptographic operation - Symmetric Encryption / Decryption

- Perform Secure messaging - encryption and decryption in accordance with a specified cryptographic algorithm AES in CBC mode and DES in CBC mode. The proprietary Infineon Secure Messaging Accelerator Class is used.

FCS_COP.1/CA_MAC (EAC/PACE) Cryptographic operation - MAC

- Perform Secure messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and Retail-MAC. The proprietary Infineon Secure Messaging Accelerator Class is used. This SFR is also used for the personalization of the TOE via the Secure Channel Protocol SCP03 of Global Platform.

FCS_COP.1/SIG_VER (EAC/PACE) Cryptographic operation - Signature verification by travel document

- Perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA. The standard Java Card API functions are used.

FCS_COP.1/AA Cryptographic operation - Signature creation by travel document

- Perform digital signature creation with RSA or ECDSA. This SFR is defined in addition to the SFRs of PPs to include the Active Authentication functionality.

FCS_RND.1 Quality metric for random numbers

- Make use of random numbers that meet the AIS 31 Class PTG.3 quality metric provided by the platform.

FIA_API.1/AA Authentication Proof of Identity - AA

- Provide the Active Authentication Mechanisms according to [ICAO_9303_1] to prove the identity of the TOE. This SFR is defined in addition to the SFRs of PPs to include the Active Authentication functionality.

FIA_UAU.1 (BAC), FIA_UAU.1/PACE (EAC/PACE) Timing of authentication

- Requires each user to be successfully identified before allowing any other TSF-mediated actions.

FIA_UAU.5 (BAC), FIA_UAU.5/PACE (EAC/PACE) Multiple authentication mechanisms

- Authentication via BAC, Symmetric Authentication, PACE, Passive Authentication, and Terminal Authentication.
- In the Personalization phase Secure Channel Protocol SCP03 of Global Platform with Personalization Agent keys.

7.1.4 F.Secure_Messaging

F.Secure_Messaging provides functions necessary to realize a secure communication channel to be used for BAC and PACE.

F.Secure_Messaging consists of the following elements:

FIA_UAU.5 (BAC), FIA_UAU.5/PACE (EAC/PACE) Multiple authentication mechanisms

- Authentication via BAC, Symmetric Authentication, PACE, Passive Authentication, and Terminal Authentication.
- In the Personalization phase Secure Channel Protocol SCP03 of Global Platform with Personalization Agent keys.

FCS_COP.1/AUTH (BAC) Cryptographic operation – Authentication

- Perform 'symmetric authentication - encryption and decryption' in accordance with a specified cryptographic algorithm Triple-DES in CBC mode.

FCS_COP.1/ENC (BAC), FCS_COP.1/PACE_ENC (EAC/PACE) Cryptographic operation - Encryption / Decryption AES/3DES

- Perform Secure Messaging - encryption and decryption in accordance with the cryptographic algorithm AES in CBC mode and 3DES in CBC mode. For PACE the PACE API of the platform is used.

FCS_COP.1/MAC (BAC), FCS_COP.1/PACE_MAC (EAC/PACE) Cryptographic operation – MAC

- Perform Secure Messaging - message authentication code in accordance with a specified cryptographic algorithm CMAC-AES and Retail-MAC. For PACE MAC verification/generation the PACE API of the platform is used.

FDP_UIT.1 (BAC), FDP_UIT.1/TRM (EAC/PACE) Data exchange integrity

- 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.
- On receipt of user data determine, whether modification, deletion, insertion and replay has occurred.

FTP_ITC.1/PACE (EAC/PACE) Inter-TSF trusted channel after PACE

- Provide a communication channel between the TOE 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.

7.1.5 F.Authentication

Because the various authentication protocols of BAC and EAC/PACE are very distinct they are handled separately in the following sections.

F.Authentication consists of the following elements:

7.1.5.1 BAC authentication

FIA_UID.1 Timing of authentication

Before the user is authenticated and on behalf of the user

- allow reading the Initialization Data in Phase 2 "Manufacturing".
- allow reading of the random identifier in Phase 3 "Personalization of the MRTD".
- allow reading of the random identifier in Phase 4 "Operational Use".
- require each user to be successfully identified before allowing any other TSF-mediated actions.

FIA_UAU.1 Timing of authentication

Before the user is authenticated and on behalf of the user

- allow reading the Initialization Data in Phase 2 "Manufacturing".

- allow reading of the random identifier in Phase 3 “Personalization of the MRTD”.
- allow reading of the random identifier in Phase 4 “Operational Use”.
- require each user to be successfully identified before allowing any other TSF-mediated actions.

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

- Prevent reuse of authentication data related to the Basic Access Control Authentication Mechanism.
- Prevent reuse of authentication data related to Authentication Mechanism based on Triple-DES.

FIA_UAU.5 Multiple authentication mechanisms

- Basic Access Control Authentication Mechanism.
- Symmetric Authentication Mechanism based on Triple-DES.
- Accept the authentication attempt as *Personalization Agent* by the Secure Channel Protocol SCP03 of Global Platform with *Personalization Agent* Keys.
- Accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

FIA_UAU.6 Re-authenticating of Terminal by the TOE

- 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.

FIA_AFL.1 Authentication failure handling

- Detect when 1 unsuccessful authentication attempt occurs related to BAC authentication.
- When the defined number of unsuccessful authentication attempts has been met, wait for an administrator configurable time greater 10 seconds between the reception of the authentication command and its processing.

FDP_ACC.1 Subset access control

- 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.

FDP_ACF.1 Security attribute based access control

- Enforce the Basic Access Control SFP to the subjects: Personalization Agent, Basic Inspection System, and Terminal.
- Enforce the Basic Access Control SFP to the objects: Data EF.DG1 to EF.DG16 of the logical MRTD, Basic Inspection System, and Terminal.
- Enforce the Basic Access Control SFP to the objects: Data in EF.COM and data in EF.SOD.
- Enforce the Basic Access Control SFP to the security attributes: Authentication status of terminals.
- Determine if the successfully authenticated Personalization Agent is allowed to write the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

- Determine if 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.
- Disallow any terminal to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.
- Disallow any terminal to read any of the EF.DG1 to EF.DG16 of the logical MRTD.
- Disallow the Basic Inspection System to read the data in EF.DG3 and EF.DG4.

FDP_UCT.1 Basic data exchange confidentiality – MRTD

- Enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure.

FDP_UIT.1 Data exchange integrity – MRTD

- 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.
- On receipt of user data determine, whether modification, deletion, insertion and replay has occurred.

FMT_SMR.1 Security roles

- Maintain the roles (1.) Manufacturer , (2.) Personalization Agent , (3) Basic Inspection System.
- Associate users with roles.

FMT_LIM.1/BAC Limited capabilities

- Limit test features capabilities so that in conjunction with “Limited availability (FMT_LIM.2/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be disclosed or manipulated, (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.

FMT_LIM.2/BAC Limited availability

- Limit test features availability so that in conjunction with “Limited capabilities (FMT_LIM.1/BAC)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be manipulated, (2) TSF data to be disclosed or manipulated, (3) software to be reconstructed, (4) substantial information about con-struction of TSF to be gathered which may enable other attacks.

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

- Restrict the ability to write the Document Basic Access Keys to the Personalization Agent.

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

- Restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none.

7.1.5.2 Terminal authentication

FIA_UAU.5/PACE Multiple authentication mechanisms

- PACE Protocol.

- Passive Authentication.
- Terminal Authentication.
- Secure messaging in MAC-ENC mode.
- Symmetric Authentication Mechanism based on Triple-DES or AES.
- Terminal Authentication Protocol.
- Authenticate user's claimed identity according to FIA_UAU.5.2/PACE.

FIA_UID.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.
- Identify user according to FIA_UID.1.2.

FDP_ACC.1/TRM Subset access control - Terminal Access

- Enforce the Access Control SFP on terminals gaining access to the User data and data stored in EF.Sod

FDP_ACF.1/TRM Security attribute based access control

- Enforce the Access Control SFP to objects based on Subjects (Terminal, BIS-PACE, Extended Inspection System), Objects (data EF.DG1, EF.DG2, and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical MRTD, data in EF.DG3 of the logical MRTD, data in EF.DG4 of the logical MRTD, all TOE intrinsic secret cryptographic keys stored in the travel document) and Security attributes (PACE Authentication,Terminal Authentication v.1, Authorization of the Terminal) according to FDP_ACF.1.1.
- Enforce the rules according to FDP_ACF.1.2 to determine if an operation among controlled subjects and controlled objects is allowed.
- Allow a BIS-PACE to read data objects from FDP_ACF.1.1/TRM after a successful PACE authentication as required by FIA_UAU.1/PACE.
- Authorize access of subjects to objects based on the following additional rules: none.
- Prevent any terminal being not authenticated as PACE authenticated BIS-PACE from reading, writing, modifying, or using any User Data stored on the travel document.
- Prevent Terminals not using secure messaging from reading, writing, modifying, or using any data stored on the travel document.
- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4(Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

- Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
- Prevent Terminals authenticated as CVCA or as DV from reading data in the EF.DG3 and EF.DG4.

FMT_MTD.3 Secure TSF data

- 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 with the following 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.

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

- Provide a communication channel between the TOE 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.
- Permit another trusted IT product to initiate communication via the trusted channel.
- Enforce communication via the trusted channel for any data exchange between the TOE and the Terminal.

7.1.5.3 Chip authentication

FIA_UID.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.

- Active Authentication Mechanism.
- Identify user according to FIA_UID.1.2.

FIA_UAU.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Identification by selection of the authentication key.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.
- Authenticate user according to FIA_UAU.1.2.

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

- Re-authenticate the user after successful run of the Chip Authentication Protocol.
- Verify commands as being sent by the Inspection System.

FIA_API.1 Authentication Proof of Identity

- Provide a Chip Authentication Protocol according to [BSI_TR-03110] to prove the identity of the TOE.

FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD

- Enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/TRM Data exchange integrity

- 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.
- On receipt of user data determine, whether modification, deletion, insertion and replay has occurred according to FDP_UIT.1.2.

7.1.5.4 Active authentication

FIA_UID.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.
- Identify user according to FIA_UID.1.2.

FIA_UAU.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Identification by selection of the authentication key.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.

- Authenticate user according to FIA_UAU.1.2.

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

- Re-authenticate the user after successful run of the Chip Authentication Protocol.
- Verify commands as being sent by the Inspection System.

FIA_API.1/AA Authentication Proof of Identity - AA

- Provide the Active Authentication Mechanisms according to [ICAO_9303_1] to prove the identity of the TOE.

FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD

- Enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/TRM Data exchange integrity

- 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.
- On receipt of user data determine, whether modification, deletion, insertion and replay has occurred according to FDP_UIT.1.2.

FCS_COP.1/AA Cryptographic operation - Signature creation by travel document

- Perform digital signature creation with RSA or ECDSA. This SFR is defined in addition to the SFRs of PPs to include the Active Authentication functionality.

7.1.5.5 Symmetric authentication

FDP_ACF.1/TRM Security attribute based access control

- Enforce the Access Control SFP to objects based on Subjects (Terminal, BIS-PACE, Extended Inspection System), Objects (data EF.DG1, EF.DG2, and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical MRTD, data in EF.DG3 of the logical MRTD, data in EF.DG4 of the logical MRTD, all TOE intrinsic secret cryptographic keys stored in the travel document) and Security attributes (PACE Authentication,Terminal Authentication v.1, Authorization of the Terminal) according to FDP_ACF.1.1.
- Enforce the rules according to FDP_ACF.1.2 to determine if an operation among controlled subjects and controlled objects is allowed.
- Allow a BIS-PACE to read data objects from FDP_ACF.1.1/TRM after a successful PACE authentication as required by FIA_UAU.1/PACE.
- Authorize access of subjects to objects based on the following additional rules: none.
- Prevent any terminal being not authenticated as PACE authenticated BIS-PACE from reading, writing, modifying, or using any User Data stored on the travel document.
- Prevent Terminals not using secure messaging from reading, writing, modifying, or using any data stored on the travel document.
- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4(Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
- Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
- Prevent Terminals authenticated as CVCA or as DV from reading data in the EF.DG3 and EF.DG4.

FIA_UAU.5/PACE Multiple authentication mechanisms

- PACE Protocol.
- Passive Authentication.
- Terminal Authentication.
- Secure messaging in MAC-ENC mode.
- Symmetric Authentication Mechanism based on Triple-DES or AES.
- Terminal Authentication Protocol.
- Authenticate user's claimed identity according to FIA_UAU.5.2/PACE.

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

- Restrict the ability to write the (1.) initial Country Verifying Certification Authority Public Key, the (2.) initial Country Verifying Certification Authority Certificate, and the (3.) initial Current Date to the Personalization Agent.

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

- Restrict the ability to update the (1.) Country Verifying Certification Authority Public Key and the (2.) Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority.

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

- Restrict the ability to modify the Current date to the (1.) Country Verifying Certification Authority, the (2.) Document Verifier, and the (3.) Domestic Extended Inspection System.

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

- Restrict the ability to load the Chip Authentication Private Key to the Personalization Agent.

7.1.5.6 PACE protocol

FIA_UID.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.
- Identify user according to FIA_UID.1.2.

FIA_UAU.1/PACE Timing of authentication

- Establish the communication channel, PACE Protocol.
- Read the Initialization Data according to FMT_MTD.1/INI_DIS.
- Identification by selection of the authentication key.
- Chip Authentication Protocol.
- Terminal Authentication Protocol.
- Active Authentication Mechanism.
- Authenticate user according to FIA_UAU.1.2.

FIA_UAU.5/PACE Multiple authentication mechanisms

- PACE Protocol.
- Passive Authentication.
- Terminal Authentication.
- Secure messaging in MAC-ENC mode.
- Symmetric Authentication Mechanism based on Triple-DES or AES.
- Terminal Authentication Protocol.
- Authenticate user's claimed identity according to FIA_UAU.5.2/PACE.

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

- Re-authenticate the user after successful run of the PACE Protocol.
- Verify commands as being sent by the terminal.

7.1.5.7 General

FPT_EMSEC.1 (BAC), FPT_EMS.1 (EAC/PACE) TOE Emanation

- Avoid emitting information about IC power consumption and command execution time in excess of non-useful information enabling access to secret data of the TOE.
- Ensure any users are unable to use the smart card circuit contacts to gain access to secret data of the TOE.
- The TOE relies on the platform service SF.Physical provided by Secora™ ID S v1.1.

7.1.6 F.Integrity

F.Integrity assures the integrity of internal applet data. It is based on the platform service SF.Physical provided by Secora™ ID S v1.1 (cf. the security target [SECORA_ST-SLJ52]).

F.Integrity consists of the following elements:

FPT_FLS.1/BAC (BAC), FPT_FLS.1 (EAC/PACE) Failure with preservation of secure state

- Preserve a secure state when the following types of failures occur:
  - Exposure to operating conditions causing a TOE malfunction.
  - Failure detected by TSF according to FPT_TST.1.

FPT_TST.1 (BAC, EAC/PACE) TSF testing

- Run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. The TOE makes use of the User Mode Security Life Control selftest provided by the platform during startup. The self test functionality is therefore realized by Secora™ ID S v1.1 and the hardware.

FPT_PHP.3 (BAC, EAC/PACE) Resistance to physical attack

- Resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

7.2 Assurance Measures

7.2.1 Assurance Measures (BAC)

The assurance measures fulfilling the requirements of EAL4 augmented with ALC_DVS.2 is given in table 7.1.

ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification 4
ADV_IMP.1	Implementation representation of the TSF 4
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

Table 7.1: Assurance Measures (BAC)

7.2.2 Assurance Measures (EAC/PACE)

The assurance measures fulfilling the requirements of EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 are given in table 7.2.

ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.1	Implementation representation of the TSF
ADV_INT.2	Well-structured internals
ADV_TDS.4	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures, automation
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.2	Compliance with implementation standards
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Table 7.2: Assurance Measures (EAC/PACE)

7.3 TOE Summary Specification Rationale

The following tables show the coverage of the SFRs by TSFs for BAC and EAC/PACE. Each SFR is covered by at least one TSF which shows that all TOE security requirements are fulfilled. Section ’7.1 TOE Security Functions’ gives a detailed description of the TSFs.

7.3.1 TOE Summary Specification Rationale (BAC)

	F.Access_Control	F.Administration	F.Crypto	F.Secure_Messaging	F.Authentication	F.Integrity
FAU_SAS.1/BAC		x				
FCS_CKM.1			x			
FCS_CKM.4			x			
FCS_COP.1/SHA			x			
FCS_COP.1/ENC				x		
FCS_COP.1/AUTH				x		
FCS_COP.1/MAC			x	x		
FCS_RND.1			x			
FIA_UID.1	x				x	
FIA_UAU.1	x				x	
FIA_UAU.4	x				x	
FIA_UAU.5	x		x		x	
FIA_UAU.6	x				x	
FIA_AFL.1	x				x	
FDP_ACC.1	x				x	
FDP_ACF.1	x				x	
FDP_UCT.1	x				x	
FDP_UIT.1	x			x	x	
FMT_SMF.1/BAC		x				
FMT_SMR.1	x	x			x	
FMT_LIM.1/BAC	x				x	
FMT_LIM.2/BAC	x				x	
FMT_MTD.1	x	x				
FMT_MTD.1/INI_ENA	x	x				
FMT_MTD.1/INI_DIS/BAC	x	x				
FMT_MTD.1/KEY_WRITE	x					
FMT_MTD.1/KEY_READ/BAC	x					
FPT_EMSEC.1					x	
FPT_FLS.1/BAC						x
FPT_TST.1						x
FPT_PHP.3						x

Table 7.3: Coverage of the SFRs by TSFs (BAC)

7.3.2 TOE Summary Specification Rationale (EAC/PACE)

SFRs and security objectives from PACE PP [CC_PP-0068-V2] are marked in *italic letters*, SFRs from PACE PP [CC_PP-0068-V2] which are extended in EAC PP [CC_PP-0056-V2] are marked in **bold letters**. SFRs and security objectives included in addition for Active Authentication are underlined.

	F.Access_Control	F.Administration	F.Crypto	F.Secure_Messaging	F.Authentication	F.Integrity
FAU_SAS.1		x				
FCS_CKM.1/CA			x			
FCS_CKM.1/DH_PACE			x			
FCS_CKM.4			x			
FCS_COP.1/CA_ENC			x			
FCS_COP.1/CA_MAC			x			
FCS_COP.1/PACE_ENC			x			
FCS_COP.1/PACE_MAC			x			
FCS_COP.1/SIG_VER			x			
FCS_COP.1/AA			x			
FCS_RND.1			x			
FIA_UID.1/PACE	x		x		x	
FIA_UAU.1/PACE	x				x	
FIA_UAU.4/PACE	x					
FIA_UAU.5/PACE	x		x	x	x	
FIA_UAU.6/PACE	x				x	
FIA_UAU.6/EAC	x				x	
FIA_AFL.1/PACE	x					
FIA_API.1					x	
FIA_API.1/AA			x			
FDP_ACC.1/TRM	x				x	
FDP_ACF.1/TRM	x				x	
FDP_RIP.1			x			
FDP_UCT.1/TRM	x				x	
FDP_UIT.1/TRM	x			x	x	
FMT_SMF.1		x				
FMT_SMR.1/PACE	x	x				
FMT_LIM.1	x	x				
FMT_LIM.2	x	x				
FMT_MTD.1/INI_ENA		x				
FMT_MTD.1/INI_DIS		x				

	F.Access_Control	F.Administration	F.Crypto	F.Secure_Messaging	F.Authentication	F.Integrity
FMT_MTD.1/CVCA_INI	x	x			x	
FMT_MTD.1/CVCA_UPD	x	x			x	
FMT_MTD.1/DATE	x	x			x	
FMT_MTD.1/AAPK	x	x				
FMT_MTD.1/CAPK	x				x	
FMT_MTD.1/KEY_READ	x					
FMT_MTD.1/KEY_READ_AA	x	x				
FMT_MTD.1/PA	x	x				
FMT_MTD.3					x	
FPT_EMS.1					x	
FPT_FLS.1						x
FPT_TST.1						x
FPT_PHP.3						x
FTP_ITC.1/PACE	x			x	x	

Table 7.4: Coverage of the SFRs by TSFs (EAC/PACE)

7.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target and the Security Target of the platform [SECORA_ST-SLJ52].

7.4.1 Mapping of the Platform TSFs

For every platform TSF the following Table 7.5 maps the corresponding TSFs of this Composite ST or shows that they are not relevant. Because the TSFs of the TOE are the same for BAC and EAC/PACE no distinction is necessary here.

Platform TSF	Corresponding TSF	Remarks
SF.Firewall	N/A (used implicitly)	Java Card applet management
SF.RIP	F.Administration, F.Integrity	Java Card TOE
SF.Rollback	F.Integrity	Java Card TOE
SF.SCP	F.Access_Control	GlobalPlatform secure channel
SF.CM	F.Access_Control	GlobalPlatform card management
SF.Physical	F.Integrity, F.Administration, F.Access_Control	Java Card TOE
SF.CS	F.Crypto, F.Access_Control, F.Administration	Java Card TOE
SF.PIN	N/A (used implicitly)	Java Card TOE

Table 7.5: Correspondence and Relevance of Platform and Composite TSFs

7.4.2 Mapping of the Platform Objectives

Some of the security objectives of the TOE and the platform can be mapped directly (see Table 7.6). None of them show any conflicts between each other. Because the objectives of the TOE are the same for BAC and EAC/PACE no distinction is necessary here.

Platform Objective	Corresponding Objective	Remarks
O.SID	N/A (used implicitly)	No conflict with this ST.
O.FIREWALL	N/A (used implicitly)	No conflict with this ST.
O.GLOBAL_ARRAYS_CONFID	OT.Data-Confidentiality OT.Sens_Data_Conf OT.Data_Conf	No conflict with this ST.
O.GLOBAL_ARRAYS_INTEG	OT.Data-Integrity OT.Data_Int	No conflict with this ST.
O.NATIVE	N/A (used implicitly)	No conflict with this ST.
O.OPERATE	N/A (used implicitly)	No conflict with this ST.
O.REALLOCATION	N/A (used implicitly)	No conflict with this ST.
O.RESOURCES	N/A (used implicitly)	No conflict with this ST.
O.ALARM	N/A (used implicitly)	No conflict with this ST.
O.CIPHER	N/A (used implicitly)	This platform objective is relevant for the correct function of the TOE because it makes use of cryptographic algorithms provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.KEY-MNGT	N/A (used implicitly)	No conflict with this ST.
O.PIN-MNGT	N/A (used implicitly)	No conflict with this ST.
O.TRANSACTION	N/A (used implicitly)	No conflict with this ST.
O.OBJ-DELETION	N/A (used implicitly)	No conflict with this ST.
O.DELETION	N/A (used implicitly)	No conflict with this ST.
O.LOAD	N/A (used implicitly)	No conflict with this ST.
O.INSTALL	N/A (used implicitly)	No conflict with this ST.
O.COMMUNICATION	N/A (used implicitly)	No conflict with this ST.
O.CARD-MANAGEMENT	N/A (used implicitly)	No conflict with this ST.
O.SCP.IC	OT.Prot_Phys-Tamper OT.Prot_Inf_Leak	No conflict with this ST.
O.SCP.RECOVERY	OT.Prot_Malfunction	No conflict with this ST.

Platform Objective	Corresponding Objective	Remarks
O.SCP.SUPPORT	N/A (used implicitly)	This platform objective is relevant for the correct function of the TOE because it makes use of cryptographic algorithms provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.
O.SCP.RNG	N/A (used implicitly)	This platform objective is relevant for the correct function of the TOE because it makes use of random numbers provided by the platform. However, there is no directly corresponding objective for the TOE. No conflict with this ST.

Table 7.6: Correspondence and Relevance of Platform and Composite Objectives

7.4.3 Mapping of the Platform SFRs

The relevant Security Requirements of the TOE and the platform can be mapped directly (see Table 7.7). None of them show any conflicts between each other.

Platform SFR	Corresponding SFR	Remarks
FDP_ACC.2/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FDP_ACF.1/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FDP_IFC.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FDP_IFF.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FDP_RIP.1/OBJECTS	N/A (used implicitly).	Java Card Firewall. No conflict.
FMT_MSA.1/JCRE	N/A (used implicitly)	Java Card Firewall. No conflict.
FMT_MSA.1/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.
FMT_MSA.2/ FIREWALL_JCVM	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FMT_MSA.3/FIREWALL	N/A (used implicitly)	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FMT_MSA.3/JCVM	N/A (used implicitly)	Java Virtual Machine. No conflict.

Platform SFR	Corresponding SFR	Remarks
FMT_SMF.1	N/A (used implicitly)	Java Card Firewall. No conflict.
FMT_SMR.1	N/A (used implicitly)	Java Card Firewall. No conflict.
FCS_CKM.1	**BAC:** FCS_CKM.1 **EAC/PACE:** FCS_CKM.1/DH-PACE FCS_CKM.1/CA	Overlapping requirements between TOE SFR and platform SFR.
FCS_CKM.2	N/A (used implicitly)	Java Card internal. No conflict.
FCS_CKM.3	N/A (used implicitly)	Java Card internal. No conflict.
FCS_CKM.4	FCS_CKM.4	TOE SFR based on platform SFR.
FCS_COP.1 with iterations **JCAPI:** FCS_COP.1.1/JCAPI/* **Global Platform SCP:** FCS_COP.1.1/SCP/* **Secure Messaging:** FCS_COP.1.1/SM/*	**BAC:** FCS_COP.1/SHA FCS_COP.1/ENC FCS_COP.1/AUTH FCS_COP.1/MAC **EAC/PACE:** FCS_COP.1/PACE_ENC FCS_COP.1/PACE_MAC FCS_COP.1/CA_ENC FCS_COP.1/CA_MAC FCS_COP.1/SIG_VER FCS_COP.1/AA FIA_UAU.5.2/PACE	**BAC:** FCS_COP.1/SHA is covered by FCS_COP.1.1/JCAPI/HASH. FCS_COP.1/ENC is covered by FCS_COP.1.1/SM/ICAO-ENC-TDES. FCS_COP.1/AUTH is covered by FCS_COP.1.1/SM/ICAO-ENC-TDES. FCS_COP.1/MAC is covered by FCS_COP.1.1/SM/ICAO-MAC-TDES. **EAC/PACE:** FCS_COP.1/PACE_ENC is covered by FCS_COP.1.1/SM/PACE. FCS_COP.1/PACE_MAC is covered by FCS_COP.1.1/SM/PACE. FCS_COP.1/CA_ENC is covered by FCS_COP.1.1/JCAPI/ECDH. FCS_COP.1/CA_MAC is covered by FCS_COP.1.1/JCAPI/ECDH. FCS_COP.1/SIG_VER is covered by FCS_COP.1.1/JCAPI/ECDSA-VER. FCS_COP.1/AA is covered by FCS_COP.1.1/JCAPI/RSA-DEC[1] and FCS_COP.1.1/JCAPI/ECDSA-SIG. FIA_UAU.5.2/PACE is covered by FCS_COP.1.1/SCP/ENC-AES and FCS_COP.1.1/SCP/MAC-AES
FDP_RIP.1/ABORT	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/APDU	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/bArray	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/KEYS	FDP_RIP.1	TOE SFR based on platform SFR.
FDP_RIP.1/TRANSIENT	N/A (used implicitly).	Java Card internal. No conflict.

[1]Because FCS_COP.1.1/JCAPI/RSA-SIG supports only SHA-1 for ISO 9796-2 the TOE instead makes use of FCS_COP.1.1/JCAPI/RSA-DEC for signature generation (SHA-2 family also supported).

Platform SFR	Corresponding SFR	Remarks
FDP_ROL.1/FIREWALL	N/A (used implicitly).	Java Card Firewall. Applet requirements are mentioned in the User Guidance. No conflict.
FAU_ARP.1	FPT_FLS.1	TOE SFR based on platform SFR.
FDP_SDI.2	FPT_FLS.1	TOE SFR based on platform SFR.
FPR_UNO.1	N/A (used implicitly)	Java Card internal. No conflict.
FPT_FLS.1	FPT_FLS.1	TOE SFR based on platform SFR.
FPT_TDC.1	N/A (used implicitly)	Java Card internal. No conflict.
FIA_ATD.1/AID	N/A (used implicitly).	Java Card internal. No conflict.
FIA_UID.2/AID	N/A (used implicitly).	Java Card internal. No conflict.
FIA_USB.1/AID	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MTD.1/JCRE	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MTD.3/JCRE	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ITC.2/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMR.1/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FPT_FLS.1/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FPT_RCV.3/Installer	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ACC.2/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_ACF.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MSA.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_MSA.3/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMF.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FMT_SMR.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FPT_FLS.1/ADEL	N/A (used implicitly).	Java Card internal. No conflict.
FDP_RIP.1/ODEL	FDP_RIP.1	TOE SFR based on platform SFR.
FPT_FLS.1/ODEL	FPT_FLS.1	TOE SFR based on platform SFR.
FDP_UIT.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ROL.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ITC.2/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FPT_FLS.1/CCM	N/A (used implicitly)	Java Card internal. No conflict.
FCS_COP.1/DAP	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ACC.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FDP_ACF.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_MSA.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_MSA.3/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_SMF.1/SD	N/A (used implicitly)	Java Card internal. No conflict.
FMT_SMR.1/SD	N/A (used implicitly)	Java Card internal. No conflict.

Platform SFR	Corresponding SFR	Remarks
FTP_ITC.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FCO_NRO.2/SC	N/A (used implicitly)	Java Card internal. No conflict.
FDP_IFC.2/SC	N/A (used implicitly)	Java Card internal. No conflict.
FDP_IFF.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_MSA.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_MSA.3/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FMT_SMF.1/SC	N/A (used implicitly)	GlobalPlatform. No conflict.
FIA_UID.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FIA_UAU.1/SC	N/A (used implicitly)	Java Card internal. No conflict.
FIA_UAU.4/SC	N/A (used implicitly)	Java Card internal. No conflict.
FPT_PHP.3	FPT_PHP.3	TOE SFR based on platform SFR.
FPT_TST.1	FPT_TST.1	TOE SFR based on platform SFR.
FCS_RNG.1	FCS_RND.1	The TOE makes use of random numbers according to AIS 31 Class PTG.3. The platform provides random numbers with the defined quality metric to be used directly.

Table 7.7: Correspondence and Relevance of Platform and Composite SFRs

7.4.4 TOE Security Environment

This Security Target considers the assumptions and objectives for the operational environment of the protection profiles [CC_PP-0055], [CC_PP-0056-V2], [CC_PP-0068-V2], and the Security Target of the platform [SECORA_ST-SLJ52].

7.4.4.1 Relevance of Platform Security Objectives for the Operational Environment

Significant Platform Security Objectives for the Operational Environment must be considered.

Platform Objective for the Environment	Relevance for Composite ST
OE.APPLET	According to OE.APPLET applets loaded post-issuance must not contain native methods. The user guidance contains respective directives.
OE.VERIFICATION	According to OE.VERIFICATION all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. The user guidance contains respective directives.
OE.CODE-EVIDENCE	According to OE.CODE-EVIDENCE for application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION. For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification. For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Security Target. All this is achieved by making use of a checksum along with respective instructions in the user guidance.

Table 7.8: Platform Security Objectives for the Operational Environment

7.4.4.2 Assurance Requirements

The level of assurance of the

- TOE-BAC is EAL4 augmented with ALC_DVS.2
- TOE-EAC/PACE is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
- JavaCard platform is EAL6 augmented with ALC_FLR.1
- Hardware (Infineon Technologies AG, IFX_CCI_000005) is EAL6 augmented

This shows that the Assurance Requirements of the TOE is matched or exceeded by the Assurance Requirements of the platform and hardware. There are no conflicts.

7.4.5 Conclusion

Overall no contradictions between the Security Targets of the TOE, the JavaCard platform and the hardware can be found.

8 Glossary and Acronyms

Accurate Terminal Certificate A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [BSI_TR-03110].

Advanced Inspection Procedure (with PACE) A specific order of authentication steps between a travel document and a terminal as required by [ICAO_SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE and EIS-AIP-BAC.

Agreement This term is used in [CC_PP-0056-V2] in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.

Active Authentication Security mechanism defined in [ICAO_9303] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organization.

Application note / Note Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalization Data.

Authenticity Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization

Basic Access Control (BAC) Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the basic inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

Basic Inspection System with PACE protocol (BIS-PACE) A technical system being used by an inspecting authority and operated by a governmental organization (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).

The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorized by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.

Basic Inspection System (BIS) An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.

Biographical data (biodata) The personalized details of the travel document holder appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO_9303]

Biometric reference data Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.

Card Access Number (CAN) Password derived from a short number printed on the front side of the data-page.

Certificate chain A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]

Country Signing CA Certificate (C_{CSCA}) Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority and stored in the inspection system.

Country Signing Certification Authority (CSCA) An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI.

The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.

The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [BSI_TR-03110].

Country Verifying Certification Authority (CVCA) An organization enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [BSI_TR-03110].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a CVCS as a subject; hence, it merely represents an organizational entity within [CC_PP-0056-V2].

The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [BSI_TR-03110].

Current date The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CV Certificate Card Verifiable Certificate according to [BSI_TR-03110].

CVCA link Certificate Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm The [ICAO_9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

PACE passwords Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO_SAC].

Document Details Data Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.

Document Security Object (SO_D) A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303]

Document Signer (DS)

Document Signer (DS) An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.

A Document Signer is authorized by the national CSCA issuing the Document Signer Certificate (C_{DS})(CDS), see [BSI_TR-03110] and [ICAO_9303].

This role is usually delegated to a Personalization Agent.

Document Verifier (DV) An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by - inter alia - issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [BSI_TR-03110].

Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity within this ST.

There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a

policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer and a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).[1],[2]

Eavesdropper A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303]

Travel document (electronic) The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

ePassport application A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [BSI_TR-03110].

Extended Access Control Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.

Extended Inspection System (EIS) A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait. [ICAO_9303]

Global Interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all travel documents. [ICAO_9303]

IC Dedicated Software Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.

[1] The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in BSI-CC-PP-0068-V2-2011 in order to reflect an appropriate relationship between the parties involved.

[2] Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.

IC Dedicated Support Software That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC Embedded Software Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.

IC Identification Data The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [ICAO_9303]

Improperly documented person A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303]

Initialization Process of writing Initialization Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).

Initialization Data Any data defined by the TOE manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are, for instance, used for traceability and for IC identification as travel document's material (IC identification data).

Inspection The act of State examining an travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO_9303].

Inspection system (IS) A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder.

Integrated circuit (IC) Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.

Integrity Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organisation.

Issuing Organization Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]

Issuing State The Country issuing the travel document. [ICAO_9303]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip.

Logical travel document Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contactless/contact-based integrated circuit. It presents contactless or contact based readable data including (but not limited to)

1. personal data of the travel document holder
2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
3. the digitized portraits (EF.DG2),
4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and
5. the other data according to LDS (EF.DG5 to EF.DG16).
6. EF.COM and EF.SOD

Machine readable travel document (MRTD) Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303].

Machine readable zone (MRZ) Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1,the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303].

The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303]

Manufacturer Generic term for the IC manufacturer producing integrated circuit and the travel document manufacturer completing the IC to the travel document. The *Manufacturer* is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC manufacturer and travel document manufacturer using this role manufacturer.

Metadata of a CV Certificate Data within the certificate body (excepting Public Key) as described in [BSI_TR-03110].

The metadata of a CV certificate comprise the following elements:

- Certificate Profile Identifier,
- Certificate Authority Reference,
- Certificate Holder Reference,
- Certificate Holder Authorization Template,
- Certificate Effective Date,
- Certificate Expiration Date.

ePassport application Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes

- the file structure implementing the LDS [ICAO_9303],

- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except the authentication data itself.

Optional biometric reference data Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication Security mechanism implementing (i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Password Authenticated Connection Establishment (PACE) A communication establishment protocol defined in [ICAO_SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.

PACE password A password needed for PACE authentication, e.g. CAN or MRZ.

Personalization The process by which the Personalization Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrollment" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).

Personalization Agent An organization acting on behalf of the travel document Issuer to personalize the travel document for the travel document holder by some or all of the following activities:

i establishing the identity of the travel document holder for the biographic data in the travel document,
ii enrolling the biometric reference data of the travel document holder,
iii writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [BSI_TR-03110],
iv writing the document details data,
v writing the initial TSF data,
vi signing the Document Security Object defined in [ICAO_9303] (in the role of DS).

Please note that the role '*Personalization Agent*' may be distributed among several institutions according to the operational policy of the travel document Issuer.

Generating signature key pair(s) is not in the scope of the tasks of this role.

Personalization Data A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and

(iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the *Personalization Agent* in the life cycle phase *card issuing*.

Pre-personalization Data Any data that is injected into the non-volatile memory of the TOE by the *Manufacturer* for traceability of the non-personalized travel document and/or to secure shipment within or between the life cycle phases *Manufacturing* and *card issuing*.

Pre-personalized travel document's chip Travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.

Receiving State The Country to which the travel document holder is applying for entry; see [ICAO_9303].

Reference data Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

RF-terminal A device being able to establish communication with an RF-chip according to ISO/IEC 14443.

Rightful equipment (rightful terminal or rightful Card) A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see *Inspection System*).

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [ICAO_9303]

Secure messaging in combined mode Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Skimming Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact-based communication channel of the TOE without knowledge of the printed PACE password.

Standard Inspection Procedure A specific order of authentication steps between an travel document and a terminal as required by [ICAO_SAC], namely (i) PACE and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.

Supplemental Access Control A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.

Terminal A Terminal is any technical system communicating with the TOE through a contactless/contact-based interface.

TOE tracing data Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognizing the travel document.

Travel document Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document").

Travel document (electronic) The contactless/contact-based smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.

Travel document holder A person for whom the ePass Issuer has personalized the travel document.

Travel document Issuer (issuing authority) Organization authorized to issue an electronic Passport to the travel document holder.

Travel document presenter A person presenting the travel document to a terminal and claiming the identity of the travel document holder.

TSF data Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC_Part1]).

Unpersonalized travel document Travel document material prepared to produce a personalized travel document containing an initialized and pre-personalized travel document's chip.

User data All data (being not authentication data)

i stored in the context of the ePassport application of the travel document as defined in [ICAO_9303] and

ii being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_SAC]).

CC give the following generic definitions for user data:
Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC_Part1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC_Part2]).

Verification data Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [CC_PP-0055])
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
CGA	Certificate generation application. In the current context, it is represented by ATT for the eSign application.
CHAT	Certificate Holder Authorization Template
DTBS	Data to be signed
DTBS/R	Data to be signed or its unique representation
EAC	Extended Access Control
EIS-AIP-BAC	Extended Inspection System with BAC (equivalent to EIS as used in [CC_PP-0056-V2])
EIS-AIP-PACE	Extended Inspection System with PACE (see [BSI_TR-03110], sec. 3.1.1, 3.2.1)
EIS-GAP	Extended Inspection System using GAP (see [BSI_TR-03110], sec. 3.1.1, 3.2.1)
GAP	General Authentication Procedure (see [BSI_TR-03110], sec. 3.4)
HID	Human Interface Device. It is equivalent to SGT in the context of ID_Card.
MRZ	Machine readable zone
N/A	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RAD	Reference Authentication Data
RF	Radio Frequency
SAC	Supplemental Access Control

Acronym	Term
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [BSI_TR-03110], sec. 3.1.1
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)

9 Bibliography

[AGD_ePP] MaskTech ePP Applet on Secora™ ID S v1.1 User Manual, MaskTech International GmbH, Version 1.08, 2022-09-08.

[BSI_AIS31] Anwendungshinweise und Interpretationen zum Schema – Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, AIS 31, Version 3, 2013-05-15.

[BSI_TR-03110] TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents, BSI, Version 2.20, 2015.

[BSI_TR-03110-1] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015-02-26.

[BSI_TR-03111] TR-03111, Technical Guideline TR-03111: Elliptic Curve Cryptography, BSI, Version 2.1, 2018-06-01.

[CC-PP-2010/03-M01] ANSSI-CC-PP-2010/03-M01, Java Card Protection Profile – Open Configuration, Oracle Corporation, Version 3.0, 2012-05.

[CC_Part1] CCMB-2017-04-001, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Common Criteria Maintenance Board, 2017-04.

[CC_Part2] CCMB-2017-04-002, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Common Criteria Maintenance Board, 2017-04.

[CC_Part3] CCMB-2017-04-003, Version 3.1, Revision 5, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Common Criteria Maintenance Board, 2017-04.

[CC_PartEM] CCMB-2017-04-004, Version 3.1, Revision 5, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, Version 3.1, Revision 5, 2017-04.

[CC_PP-0055] BSI-CC-PP-0055-2009, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Basic Access Control, BSI, Version 1.10, 2009-03-25.

[CC_PP-0056] BSI-CC-PP-0056-2009, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control, BSI, Version 1.10, 2009-03-25.

[CC_PP-0056-V2] BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile / Machine Readable Travel Document with 'ICAO Application', Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05.

[CC_PP-0068-V2] BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (ePass_PACE PP), BSI, Version 1.01, 2014-07-22.

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard (SHS), National Institute of Standards and Technology, 2015-08.

[FIPS_197] FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), National Institute of Standards and Technology, 2001-11.

[GP] GPC_SPE_034, GlobalPlatform Card - Card specification Version 2.3.1, GlobalPlatform, March 2018.

[GP_SCP03] GPC_SPE_014, GlobalPlatform Technology - Secure Channel Protocol '03' - Card Specification v2.3 - Amendment D - Version 1.2, GlobalPlatform, April 2020.

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2021.

[ICAO_9303_1] ICAO Doc 9303, Machine Readable Travel Documents: Part 1 – Introduction, ICAO, 2021.

[ICAO_SAC] Technical Report: Supplemental Access Control for Machine Readable Travel Documents, ICAO, TR-SAC V1.1, 2014-04-15.

[ISO_11770-3] ISO/IEC 11770-3:2021, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, ISO/IEC, 2021-10-01.

[ISO_14443] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Multipart Standard, ISO/IEC, 2016-2018.

[ISO_7816-3] ISO/IEC 7816-3:2006, Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols, ISO/IEC, 2006-10.

[ISO_9796-2] ISO/IEC 9796-2:2010, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO/IEC, 2010-12.

[ISO_9797] ISO/IEC 9797, Information technology – Security techniques – Message Authentication Codes (MACs) – Multipart Standard, ISO/IEC, 1999, 2002.

[NIST_SP800-38A] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology, 2001-12.

[NIST_SP800-67] NIST SP 800-67 Rev. 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST, 2017-11.

[SC_HID] BSI-DSZ-CC-S-0183-2021, HID Global GmbH, Site Security Target Lite of HID Global Ireland Teoranta in Galway, Ireland, Doc. No: F-10-138d, Rev. B, 2018-09-13.

[SC_HID_MY] BSI-DSZ-CC-S-0189-2021, HID Global GmbH, Site Security Target Lite for HID Global Malaysia, PRO-01286 Rev D2, 2020-04-17.

[SC_Linxens] BSI-DSZ-CC-S-0207-2021, Linxens (Thailand) Co Ltd., Site Security Target LITE for Linxens Thailand, Version 2.4, 2021-11-24.

[SECORA_ST-SLJ52] Infineon Technologies AG, Secora™ ID S v1.1 (SLJ52GxxyyyzS) Security Target.

10 Revision History

Version	Date	Author	Changes
1.0	2022-06-07	Thomas Rölz	Initial version
1.1	2022-08-24	Thomas Rölz	Updated bibliography
1.2	2022-09-09	Thomas Rölz	Updated bibliography

11 Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 5
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de