MK Lotus GovID IMDa in EAC with PACE Configuration

Security Target Lite

MK Lotus GovID IMDa V4.6.8.8 - Extended Access Control with PACE

Common Criteria Evaluation Assurance Level 5+

December 12th, 2025

Revision 1.0

Table of Contents

List of Tables

Abbreviations and Notations

Numerical values
Numbers are printed in decimal, hexadecimal or binary notation.
Hexadecimal values are indicated with a ‘h’ suffix as in XXh, where X is a hexadecimal digit from 0 to F.
Decimal values have no suffix.

Example: the decimal value 179 may be noted as the hexadecimal value B3h.

Denoted text
The text added to provide details on how the TOE implementation fulfils some security requirements is preceded by the numbered tag “Application Note”.

Key words
The words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” are to be interpreted as described in RFC2119 [1].

1. Introduction

1.1. ST overview

This Security Target defines the security objectives and requirements for the contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment (PACE), Extended Access Control (EAC), Passive Authentication (PA) and Chip Authentication similar to the Active Authentication in 'ICAO Doc 9303' [2] [3] [4].

This ST addresses the following advanced security mechanisms featured by the ICAO application:

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 8th ed. Part 11 [3], and Terminal Authentication according to BSI TR-03110 [5] [6],
- Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 8th ed. Part 11 [3], and
- Active Authentication according to ICAO Doc 9303 8th ed. Part 11 [3].

The ePassport product also supports Basic Access Control (BAC) compliant with ICAO Doc 9303 [3], addressed by another ST [7].

1.2. ST reference

Table 1 ST identification

Title	Security Target Lite - MK Lotus GovID IMDa V4.6.8.8 – Extended Access Control with PACE
Version	1.0
Date	2025-12-12
Authors	MK Smart

1.3. TOE reference

Table 2 TOE identification

TOE Name	MK Lotus GovID IMDa in EAC with PACE Configuration
TOE Version	V4.6.8.8
TOE identifier	Lotus GovID IMDa V4.6.8.8
TOE Identification Data	47h 4Fh 56h 2Dh 4Dh 4Bh 34h 2Eh 36h 2Eh 38h 2Eh 38h
Developer	MK Smart JSC
Evaluation Sponsor	MK Smart JSC
Evaluation Facility	Applus+ Laboratories

The TOE is delivered as a chip ready for loading of applications. It is identified by the following string, representing the Global Reference:

(ASCII codes 47h 4Fh 56h 2Dh 4Dh 4Bh 34h 2Eh 36h 2Eh 38h 2Eh 38h)

The TOE identification data are in the non-volatile memory of the chip. Instructions for reading identification data are provided by the guidance documentation.

1.4. TOE overview

1.4.1. TOE definition

The Target of Evaluation (TOE) addressed by the current Security target is an electronic travel document representing a contactless smart card programmed according to ICAO Docs 9303 [2] [3] [4], and additionally providing the Extended Access Control according to the BSI TR-03110 [5] [6]. 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), BSI-CC-PP-0068-V2 [8].

The TOE comprises of at least:

- the circuitry of the travel document's chip (the integrated circuit, IC), see Appendix A
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software, such as RF contactless library or Crypto library form an IC provider.
- the IC Embedded Software,
- the MRTD application with native acceleration APIs, and
- the associated guidance documentation.

1.4.2. TOE major security features for operational use

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 in case of contactless 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.

For this Security Target, the travel document is viewed as unit of:

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

(a) the biographical data on the biographical data page of the travel document surface,

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

(c) the printed portrait.

(ii) the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [2] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the travel document holder:

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

(b) the digitized portraits (EF.DG2),

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

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

(e) the Document Security Object (SOD).

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) [2] [3] [4]. 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.

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. This Security Target addresses the Chip Authentication Version 1 described in [5] and the Active Authentication stated in [3].

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) [8]'. Note that [8] considers high attack potential.

For the PACE protocol according to [3], the following steps shall be performed:

(i) 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.

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

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

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token. After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [3] and [5].

The EAC PP requires the TOE to implement the Extended Access Control as defined in [5]. 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 Organisation 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 Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

1.4.3. TOE type

The TOE type is an electronic travel document representing a contactless smart card programmed according to ICAO Doc 9303 [2] [3] [4], and BSI TR-03110 (*ePassport* application) [5] [6].

1.4.4. TOE life cycle

The TOE life-cycle is described in terms of the four life-cycle phases (subdivided into 7 steps).

Phase 1 "Development"

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software (Cryptolibraries) and the guidance documentation associated with these TOE components.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

The IC Embedded Software and MRTD application are securely delivered to the Inlay&MRTD manufacturer. The IC Embedded Software and MRTD application are loaded to the IC at the Inlay&MRTD manufacturer, the inlay and the guidance documentation is securely delivered to the personalization agent.

Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing. The IC manufacturer also performs the IC encapsulation and the delivery process to the Inlay&MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the Inlay&MRTD manufacturer.

The Inlay&MRTD manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance FLASH).

(Step4 Optional) The Inlay&MRTD manufacturer combines the IC with hardware (e.g. paper, antenna, cover material) for the contactless interface in the passport cover.

(Step5) The Inlay&MRTD manufacturer creates the MRTD application and equips MRTD's chips with pre-personalization Data.

Application Note 1 Creation of the application implies: the Applet instantiation.

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

Phase 3 "Personalization of the travel document"

(Step6) The personalization of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrolment 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.

(Optional step) The personalization agent combines the IC with hardware (e.g. paper, antenna, cover material) for the contactless interface in the passport cover.

The signing of the Document security object by the Document signer [1] and [2] 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.

Application Note 2 The passport book can be made by the Inlay&MRTD manufacturer in phase 2 or the personalization agent in phase 3.

Application Note 3 The TSF data (data created by and for the TOE, that might affect the operation of the TOE) comprise (but are not limited to) the Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

Application Note 4 This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [2] *and* [3]*. This approach allows but does not enforce the separation of these roles.*

Phase 4 "Operational Use"

(Step7) 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.

Application Note 5 The intention of the EAC PP [9] and PACE PP [8] is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organisation. In this case the national body of the issuing State or Organisation is responsible for these specific production steps. Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organisation. All production, generation and installation procedures after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore, the Security Target outlines the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.

The TOE delivery occurs at the end of phase 2 (after pre-personalization).

Table 3 Developer Roles and Actors involved in TOE Life Cycle

Roles	Actors	Phase/Step(s)	Site Identification
IC developer	Infineon	1/1: Development of IC and IC dedicated software	**Infineon Neubiberg R&D** Am Campeon 1-12 85579 Neubiberg Germany
Software developer	MK Smart JSC	1/2: Development and testing of IC Embedded Software (OS) and MRTD application	**MKSmart Factory** Lot 40, Quang Minh Industrial Zone, Me Linh District, Hanoi City, Vietnam.
IC manufacturer	Infineon Technologies AG	2/3: IC manufacturing	**Infineon Singapore Production** Global foundries fab 7, Singapore

Roles	Actors	Phase/Step(s)	Site Identification
		2/3: IC encapsulation	**Infineon Wuxi Production** No.8 Xing Chuang san lu, Singapore Industrial Park, Wuxi, Jiangsu Province, P.R.China **Infineon Regensburg Production** Wernerwerkstr.2 93049 Regensburg Germany
Inlay&MRTD manufacturer	MK Smart JSC	2/4: Embedding of IC with hardware (Optional, see the Application Note 2) 2/5: Loading of OS, MRTD application into chip, and pre-personalization	**MKSmart Factory** Lot 40, Quang Minh Industrial Zone, Me Linh District, Hanoi City, Vietnam.

Note: The IC encapsulation can be conducted by the IC manufacturer at different production sites. The Inlay&MRTD manufacturer will receive the IC module from either Infineon Wuxi Production or Infineon Regensburg Production.

1.4.5. Non-TOE hardware/software/firmware

The TOE is defined to comprise the chip and the complete operating system and application. 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, in which the antenna is made of pure copper with 0.1mm wire diameter, nevertheless these parts are not inevitable for the secure operation of the TOE.

2. TOE Description

2.1. Physical scope of the TOE

The TOE is comprised of the following parts:

- dual-interface chip IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001 (cf. Appendix A for more details);
- smart card operating system (MK Lotus GovID IMDa in EAC with PACE Configuration, v4.6.8.8) with its Runtime Environment;
- an International Civil Aviation Organization (ICAO) application (ePassport Applet Information v1.8) compliant with ICAO Doc 9303 [2] [3] [4];
- guidance documentation in PDF or excel format, example scripts and certificates about the preparation and use of the ICAO application, composed by:

Document	Version	Date	Hash value (SHA256)
ICAO Applet Personalization Guide – Additional Information [10]	1.3	2025-08-21	B244C0F4D31D4F4F635785AAEE2861EB5C79630B12E9C8F8DA02EED167D03D96
ePassport Applet Information [11]	1.8	2025-08-08	A64FC1394E2A5237B57E81007375288CA4F85139FE6B357CD2D06AC3076807DE
Operational User Guidance [12]	1.8	2025-12-04	D515ABC2CEFB35AAD6C55D09E90BC40ABD0B86CFDA380F0975D0D5691CD84A5E
Preparative Procedures [13]	1.9	2025-12-04	DF80A6796B40E94DCD77E87D20E6D46C9F08B75D4AEDD4DC9950412035D5C86A
scripts_v1.4_20250724.zip	1.4	2025-07-24	39F4EAA5BC85B4F6D39067AA1E08BAD17595AA4807B36F6B7E6F4374C69F5F15

The example scripts and example certificates are delivered in conjunction with the guidance documents to the Personalization Agent for testing purpose. The delivery method for documentation, script files and certificate files are a PGP encrypted and signed format from MK Smart secure lab through email or FTP.

The ICAO application and the OS are loaded on the Infineon chip by Inlay&MRTD manufacturer and delivered to the personalization agent through courier. The chip is delivered in form of IC module or passport book depending on whether the Phase2-Step4 is performed by the Inlay&MRTD manufacturer (see details in section 1.4.4 TOE life cycle).

The ePassport product supports both BAC and PACE operation modes, in which BAC mode as described in another ST is using as the fallback mechanism and PACE mode as described in the current ST is the default operation mode.

2.2. Logical scope of the TOE

The operating system manages all the resources of the integrated circuit that equips the e-Document, providing secure access to data and functions.
In more detail, in each life cycle phase/step, access to data and functions is restricted by means of cryptographic mechanisms as follows:

- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on GlobalPlatform SCP03 protocol.
- In phase 4, Operational use, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2, and DG5 to DG16, by means of the PACE mechanism compliant to ICAO Doc 9303-11 [3]. Access to sensitive data, i.e. DG3 and DG4, is allowed after the genuineness of the IC has been proven by means of the Chip Authentication mechanism defined in [3], and after the user has proven his/her entitlement by means of the Terminal Authentication mechanism as defined in [5]. The IC can prove the identity of itself to the user by means of the Active Authentication mechanism compliant to ICAO Doc 9303-11 [3].

After a successful authentication, the communication between the e-Document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification [14].

The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism defined in [3]. The Active Authentication mechanism defined in [3] can be used as an alternative technique to ascertain the genuineness of the chip. However, access to sensitive data requires the use of the Chip Authentication mechanism. Passive Authentication, PACE, Active Authentication, Chip Authentication, and EAC mechanisms are described in more detail in the following subsections.

2.2.1. Passive authentication

Passive Authentication consists of the following steps [3]:

1. The inspection system reads the Document Security Object (SOD), which contains the Document Signer Certificate (CDS, cf. [1]), from the IC.
2. The inspection system builds and validates a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SOD) according to [3].
3. The inspection system uses the verified Document Signer Public Key (KPuDS) to verify the signature of the Document Security Object (SOD).
4. The inspection system reads relevant data groups from the IC.
5. The inspection system ensures that the contents of the data groups are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SOD).

2.2.2. Password Authenticated Connection Establishment (PACE)

PACE is a password-authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the e-Document chip and the inspection system (i.e. the e-Document chip and the inspection system share the same password).

PACE establishes secure messaging between an e-Document chip and an inspection system based on possibly weak (short) passwords. The security context is established in the Master File. The protocol enables the e-Document chip to verify that the inspection system is authorized to access stored data, and has the following features:

- Strong session keys are provided independently of the strength of the password.
- The entropy of the password used to authenticate the inspection system can be very low (e.g. 6 digits are sufficient in general).

PACE supports, as part of the protocol execution, different mappings of the generator of the cryptographic group contained in the selected domain parameters into an ephemeral one.

The following mappings are supported by the TOE:

- *Generic Mapping*, based on a Diffie-Hellman key agreement;
- *Integrated Mapping*, based on a direct mapping of a nonce into an element of the cryptographic group;
- *Chip Authentication Mapping*, which extends the Generic Mapping and integrates Chip Authentication into the PACE protocol.

The following standardized domain parameters specified in ICAO Doc 9303-11 [3] are supported for PACE authentication with ECDH and included in the evaluation scope, including

- NIST P-224 (secp224r1)
- NIST P-256 (secp256r1)
- NIST P-384 (secp384r1)
- NIST P-521 (secp521r1)
- BrainpoolP224r1
- BrainpoolP256r1
- BrainpoolP320r1
- BrainpoolP384r1
- BrainpoolP512r1

Note: The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. These curves are included in the evaluation scope for compatibility with ePassport application standards.

The TOE supports PACE with the key agreement algorithm ECDH to generate the session keys for secure messaging:

- Triple-DES key of 112 bit in Retail-MAC mode
- AES key of 128, 192, 256 bit in CMAC mode

The key derivation function specified in ICAO Doc 9303-11 [3] is used, which requires using the hash function SHA-1 to derive the 112 bit Triple-DES key and 128 bit AES key, or the hash function SHA-256 to derive 192, 256 bit AES key.

Note: Triple-DES algorithm with 112 bit key size and Retail MAC are already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. The hash function SHA-1 is required for key derivation, which is also deprecated according to SOG-IS ACM [15]. Triple-DES used in Retail mode and SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.

2.2.3. Active Authentication

Active Authentication authenticates the IC by signing a challenge sent by the inspection system with a private key known only to the IC (cf. [3]).

For this purpose, the IC contains its own Active Authentication key pair (KPrAA and KPuAA). A hash representation of Data Group 15 (public key info, KPuAA) is stored in the Document Security Object (SOD), and is therefore authenticated by the issuer's digital signature. The corresponding private key (KPrAA) is stored in the IC secure memory.

By authenticating the Document Security Object (SOD) and Data Group 15 by means of Passive Authentication (cf. section 2.2.1) in combination with Active Authentication, the inspection system verifies that the Document Security Object (SOD) has been read from a genuine IC.

In accordance with ICAO Doc 9303 [3], the ICAO application supports signature creation compliant with ISO/IEC 9796-2 [16], Digital Signature Scheme 1 for Active Authentication, with hash algorithm SHA-256 compliant with FIPS PUB 180-4 [17] and RSA-CRT keys of 2048, 3096 and 4096 bits.

Note: Following SOG-IS ACM [15], the RSA CRT algorithm with key sizes from 1900 bits to 2999 bits is legacy. The current expiration date for the legacy use of keys from 1900 bits to 2999 bits is until 31st December 2025. The RSA-CRT algorithm with key size 2048 bits is in the evaluation scope for compatibility with ePassport application standards. However, key size of 3096 and 4096 bits is recommended.

2.2.4. Chip Authentication

Chip Authentication is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the e-Document chip (cf. [3]).

The main differences with respect to Active Authentication are:

- Challenge Semantics is prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the e-Document chip, this protocol also provides strong session keys.

Details on Challenge Semantics are described in [3].

The static Chip Authentication key pair(s) must be stored on the e-Document chip. In more detail:

- The private key is stored securely in the e-Document chip’s memory.
- The public key is stored in Data Group 14.

The protocol provides implicit authentication of both the e-Document chip itself and the stored data by performing secure messaging with the new session keys:

- Triple-DES key of 112 bit in Retail-MAC mode
- AES key of 128, 192, 256 bit in CMAC mode

The key derivation function specified in ICAO Doc 9303-11 [3] is used, which requires using the hash function SHA-1 to derive the 112 bit Triple-DES key and 128 bit AES key, or the hash function SHA-256 to derive 192, 256 bit AES key.

Note: Triple-DES algorithm with 112 bit key size and Retail MAC are already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. The hash function SHA-1 is required for key derivation, which is also deprecated according to SOG-IS ACM [15]. Triple-DES used in Retail mode and SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.

In accordance with ICAO Doc 9303 [3], the ICAO application supports Diffie-Hellman key agreement for Chip Authentication on elliptic curve groups over prime fields (ECDH algorithm, cf. [18]):

- NIST P-224 (secp224r1)
- NIST P-256 (secp256r1)
- NIST P-384 (secp384r1)
- NIST P-521 (secp521r1)
- BrainpoolP224r1
- BrainpoolP256r1
- BrainpoolP320r1
- BrainpoolP384r1
- BrainpoolP512r1

Note: The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. These curves are included in the evaluation scope for compatibility with ePassport application standards.

Chip Authentication may be performed either as a distinct protocol, or as part of the PACE protocol in case Chip Authentication Mapping is used. In the latter case, only ECDH may be used as key agreement algorithm.

2.2.5. Extended Access Control

Extended Access Control is a security mechanism by means of which the e-Document chip authenticates the inspection systems authorized to read the optional biometric reference data and protects access to these data.

The ICAO application enforces Extended Access Control through the support of Terminal Authentication v1, which is a challenge-response protocol that provides explicit unilateral authentication of the terminal.
This protocol enables the e-Document chip to verify that the terminal is entitled to access sensitive data. Terminal Authentication also authenticates the ephemeral public key chosen by the terminal to set up secure messaging through Chip Authentication (cf. section 2.2.4) or PACE with Chip Authentication Mapping (cf. section 2.2.2). In this way, the e-Document chip binds the terminal's access rights to the secure messaging session established by the authenticated ephemeral public key of the terminal.

In more detail, the terminal sends to the e-Document chip a certificate chain that starts with a certificate verifiable with a trusted public key stored on the chip, and ends with the terminal certificate. Then, the terminal signs a plaintext containing its ephemeral public key with the private key associated to its certificate, and sends the resulting signature to the e-Document chip, which authenticates the terminal by verifying the certificates and the final signature.
The read access rights to biometric data groups granted by the authentication are encoded in the certificates. Access to Data Group 3 alone, Data Group 4 alone, or both Data Group 3 and Data Group 4 may be granted.

In accordance with ICAO Doc 9303 [3], the ICAO application supports Terminal Authentication with signature verification algorithm ECDSA with SHA-224, SHA-256, SHA-384, SHA-512. The bit length of the curve shall be 224, 256, 320, 384 or 512, including:

- NIST P-224 (secp224r1)
- NIST P-256 (secp256r1)
- NIST P-384 (secp384r1)
- BrainpoolP224r1
- BrainpoolP256r1
- BrainpoolP320r1
- BrainpoolP384r1
- BrainpoolP512r1

Note: The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. The hash function SHA-224 is identified as legacy by SOG-IS ACM [15], which current expiration date is until 31st December 2025. These curves and SHA-224 are included in the evaluation scope for compatibility with ePassport application standards.

3. Conformance Claims

3.1. Common Criteria Conformance Claim

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017 [19].
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017 [20]; as follows: **Part 2 extended**.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017 [21]; as follows: **Part 3 conformant**.

3.2. Protection Profile Conformance Claim

This ST claims **strict** conformance to the following protection profiles:

- Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01 (Version 1.01, 22th July 2014) [8]
- Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 (Version 1.3.2, 05th December 2012) [9]

3.3. Package Conformance Claim

This Security Target claims conformance to:

- EAL 5 assurance package augmented by ALC_DVS.2 and AVA_VAN.5 defined in the CC part 3 [21]

3.4. Conformance Claim Rationale

This ST adopts as a reference the ICAO Doc 9303 Eighth Edition 2021. This new version includes the specification of the PACE protocol, and no longer uses the terms "Supplemental Access Control" and "SAC". Due to this update, in this ST:

- any references to the ICAO Doc 9303 2006 specification in the EAC PP [9] and in the PACE PP [8] have been replaced with references to Doc 9303 2021 Eighth Edition,
- any references to the ICAO "Supplemental Access Control" specification have been replaced with references to Doc 9303 2021 Eighth Edition,
- the terms "Supplemental Access Control" and "SAC" in the PACE PP have been replaced with the terms "Password Authenticated Connection Establishment" and "PACE".

This ST adds some notes to warn that usage of the algorithm Triple-DES and of the hash function SHA-1 is deprecated for PACE, Chip Authentication and Terminal Authentication.

The security problem definition includes the assets, the subjects, the assumptions, the threats, and the organizational security policies of both PPs (PACE PP [8] and EAC PP [9]).

The security objectives for the TOE and security objectives for the operational environment of both PPs (PACE PP [8] and EAC PP [9]) are included in this ST.

The following table shows the changes and additions made to the security objectives:

Element	Definition	Rationale
OT.Active_Auth_Proof	Proof of travel Document's chip authenticity by Active Authentication	Added to cover the proof of IC authenticity for Basic Inspection Systems.
OE.Active_Auth_Key_Document	Travel document Active Authentication key	Added to cover the generation, signature and storage of the Active Authentication key pair, as well as the support to the Inspection System.

The security functional requirements described in section 7 of this ST include the SFRs of both PACE PP [8] and EAC PP [9].

The following table shows the changes and additions made to the security functional requirements:

Element	Rationale
FIA_API.1/AA	**Iteration** This iteration has been added to cover the proof of identity by means of Active Authentication.
FIA_API.1/CA	**Iteration** This iteration replaces the original SFR FIA_API.1 from the EAC PP [9] to remark that it refers to Chip Authentication and to better distinguish it from the other iteration related to Active Authentication (FIA_API.1/AA).
FCS_COP.1/AA_SIGN	**Iteration** This iteration has been added to cover the signature of Active Authentication data.
FMT_MTD.1/AAPK	**Iteration** This iteration has been added to restrict the ability to cover the writing of the Active Authentication private key.
FPT_EMS.1.2	**Refinement** A refinement has been added to better specify access to data through circuit contacts.
FCS_CKM.1/SCP	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.

Element	Rationale
FCS_COP.1/SCP_ENC	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.
FCS_COP.1/SCP_MAC	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.
FCS_COP.1/SCP_KEY_DEC	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.
FIA_UID.1/SCP	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.
FIA_UAU.1/SCP	**Iteration** This iteration has been added to cover the secure communication through Secure Channel Protocol.
FMT_MTD.1/KEY_READ	**Refinement** This SFR is refined to restrict the ability to read the Active Authentication private key.
FCS_COP.1/SHA	**Iteration** This iteration has been added to cover the hash functions used in different protocols.

4. Security Problem Definition

4.1. Introduction

4.1.1. Assets

Due to strict conformance to both EAC PP [9] and PACE PP [8], this ST includes, as assets to be protected, all assets listed in section 3.1 of those PPs.

Assets described in PACE PP [8] are included in Table 4 and Table 5.

Table 4 Primary assets from PACE PP [8]

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	**User data stored on the TOE**	All data (being not authentication data) stored in the context of the *ePassport* application of the travel document as defined in [3] and being allowed to be *read out* solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [3]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [22].	Confidentiality Integrity Authenticity
2	**user data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)**	All data (being not authentication data) being transferred in the context of the *ePassport* application of the travel document as defined in [3] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [3]). User data can be received and sent (exchange = {receive, send}).	Confidentiality Integrity Authenticity
3	travel document tracing data	Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.	Unavailability

Application Note 6 Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the travel document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current ST also secures these specific travel document holder's data as stated in the table above.

All these primary assets represent User Data in the sense of the CC.

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are listed in the following table:

Table 5 Secondary assets from PACE PP

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
4	Accessibility to the TOE functions and data only for authorized subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorized subjects only.	Availability
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers 'Authenticity of the MRTD's chip' in [22].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	travel document communication establishment authorization data	Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as authorized user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

Application Note 7 Since the travel document does not support any secret travel document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

Application Note 8 Travel document communication establishment authorization data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorization attempt. The TOE shall secure the reference information as well as – together with the terminal connected (i.e. the input device of the terminal) – the verification information in the 'TOE ↔ terminal' channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be send to the TOE.

The secondary assets represent TSF and TSF-data in the sense of the CC.

Additional assets are defined in the EAC PP [9]:

Logical travel document sensitive User Data

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

Application Note 9 Due to interoperability reasons the 'ICAO Doc 9303' [3] *requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC (out of the scope of the current TOE). Note that the BAC mechanism cannot resist attacks with high attack potential (cf.* [22]*). If supported by the product, it is therefore recommended to use PACE (TOE's feature) instead of BAC (out of the scope of current TOE).*

Authenticity of the travel document's chip
The authenticity of the travel document's chip personalized by the issuing State or Organization for the travel document holder is used by the traveler to prove his possession of a genuine travel document.

4.1.2. Subjects and external entities

This security target considers the subjects defined in the PACE PP [8] and in the EAC PP [9].

The subjects considered in accordance with the PACE PP [8] are listed in the following table:

Table 6 Subjects and external entities from PACE PP [8]

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalized the travel document. This entity is commensurate with 'MRTD Holder' in [22]. Please note that a travel document holder can also be an attacker (s. below).
2	-	travel document presenter (traveller)	A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveler' in [22]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless interface. The role 'Terminal' is the default role for any terminal being recognized by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [22].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority (i.e. control officer) 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). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.
5	-	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 (CDS), see [2] and [3]. This role is usually delegated to a Personalization Agent.
6	-	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 document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate having to be distributed by strictly secure diplomatic means, see [3].

External Entity No.	Subject No.	Role	Definition
7	4	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 [2] and [3], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in (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. This entity is commensurate with 'Personalization agent' in [22].
8	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the Inlay&MRTD 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 Inlay&MRTD Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [22].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most *high* attack potential. Please note that the attacker might 'capture' any subject role recognized by the TOE. This external entity is commensurate with 'Attacker' in [22].

Application Note 10 Since the TOE does not use BAC, a Basic Inspection System with BAC (BIS-BAC) cannot be recognised by the TOE. The subject "Basic Inspection System with BAC" (BIS-BAC) is described in another ST.

In addition to the subjects defined by the PACE PP, this ST considers the following subjects defined by the EAC PP [9]:

Country Verifying Certification Authority

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document

Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

Document Verifier

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

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

Inspection system (IS)

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

The **Extended Inspection System (EIS)** performs the Advanced Inspection Procedure and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) Implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [4] and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

Attacker

Additionally to the definition from PACE PP [8] (chap 3.1) the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document.

Application Note 11 An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged travel document. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

4.2. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE's in use in the operational environment.

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

4.2.1. T.Skimming

Skimming travel document / Capturing Card-Terminal Communication

Adverse action: An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE.

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

Asset: confidentiality of logical travel document data

Application Note 12 A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

Application Note 13 MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. ***OE.Travel_Document_Holder****.*

4.2.2. T.Eavesdropping

Eavesdropping on the communication between the TOE and the PACE terminal

Adverse action: An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the *user data transferred between the TOE and the terminal connected*.

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

Asset: confidentiality of logical travel document data

Application Note 14 A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

4.2.3. T.Tracing

Tracing travel document

Adverse action: An attacker tries to gather *TOE tracing data* (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE.

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

Asset: privacy of the travel document holder

Application Note 15 A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST.

4.2.4. T.Forgery

Forgery of Data

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

Threat agent: having high attack potential

Asset: integrity of the travel document

4.2.5. T.Abuse-Func

Abuse of Functionality

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the *User Data stored in the TOE*, (ii) to manipulate or to disclose the *TSF-data stored in the TOE* or (iii) to manipulate (bypass, deactivate or modify) *soft-coded security functionality of the TOE*. This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the travel document holder.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document.

Application Note 16 Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

4.2.6. T.Information_Leakage

Information Leakage from travel document

Adverse action: An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential *User Data* or/and *TSF-data stored on the travel document* or/and *exchanged between the TOE*

and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Threat agent: having high attack potential

Asset: confidentiality of User Data and TSF-data of the travel document

Application Note 17 Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

4.2.7. T.Phys-Tamper

Physical Tampering

Adverse action: An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

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

Application Note 18 Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

4.2.8. T.Malfunction

Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting

errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation.

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

*Application Note 19 A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat **T.Phys-Tamper**) assuming a detailed knowledge about TOE's internals.*

4.2.9. T.Read_Sensitive_Data

Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.
The attack **T.Read_Sensitive_Data** is similar to the threat **T.Skimming** in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.
Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document.

Asset: confidentiality of logical travel document sensitive user data (i.e. biometric reference).

4.2.10. T.Counterfeit

Counterfeit of travel document chip data

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document.
The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents.

Asset: authenticity of user data stored on the TOE.

4.3. Organizational Security Policies

The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operation.

4.3.1. P.Manufact

Manufacturing of the travel document's chip
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The Inlay&MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

4.3.2. P.Pre-Operational

Pre-operational handling of the travel document

1.) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.

2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.

3.) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase.

4.) If the travel document Issuer authorizes a Personalization Agent to personalize the travel document for travel document holders, the travel document Issuer has to ensure that the Personalization Agent acts in accordance with the travel document Issuer's policy.

4.3.3. P.Card_PKI

PKI for Passive Authentication (issuing branch)

Application Note 20 The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1.) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate.

2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate having to be made available to the travel document Issuer by strictly secure means, see [3]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [3].

3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

4.3.4. P.Trustworthy_PKI

Trustworthiness of PKI

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

4.3.5. P.Terminal

Abilities and trustworthiness of terminals

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

1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [3] and [4].

2.) They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order [3]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3.) The related terminals need not to use any own credentials.

4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document [2]).

5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

4.3.6. P.Sensitive_Data

Privacy of sensitive biometric reference data

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

document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

4.3.7. P.Personalization

Personalization of the travel document by issuing State or Organization only

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

4.4. Assumptions

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

4.4.1. A.Passive_Auth

PKI for Passive Authentication
The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [3].

4.4.2. 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 [3] and/or BAC [22]. BAC may only be used if supported by the TOE[1]. 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.

[1] BAC is out of the scope in the current TOE

Justification: The assumption **A.Insp_Sys** does not confine the security objectives of the PACE PP [8] as it repeats the requirements of **P.Terminal** and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

4.4.3. A.Auth_PKI

PKI for Inspection Systems

The issuing and receiving States or Organizations 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 Organizations 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 Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

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 PACE PP [8] 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.

5. Security Objectives

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

5.1. Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

5.1.1. OT.Data_Integrity

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorized modification (physical manipulation and unauthorized modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

5.1.2. OT.Data_Authenticity

Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side[2]. The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[3].

5.1.3. OT.Data_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

5.1.4. OT.Tracing

Tracing travel document

[2] verification of SOD

[3] secure messaging after the PACE authentication, see also [2]

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

5.1.5. OT.Prot_Abuse-Func

Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

5.1.6. OT.Prot_Inf_Leak

Protection against Information Leakage

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document:

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

Application Note 21 This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

5.1.7. OT.Prot_Phys-Tamper

Protection against Physical Tampering

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

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

5.1.8. OT.Prot_Malfunction

Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment*.

5.1.9. OT.Identification

Identification of the TOE

The TOE must provide means to store Initialization[4] and Pre-Personalization Data in its non-volatile memory. The Initialization Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

5.1.10. OT.AC_Pers

Access Control for Personalization of logical MRTD

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [2] [3] and the TSF data can be written by authorized Personalization Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.

Application Note 22 The **OT.AC_Pers** implies that the data of the LDS groups written during personalization for travel document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization.

5.1.11. OT.Sens_Data_Conf

Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organization. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

[4] amongst other, IC Identification data

5.1.12. OT.Chip_Auth_Proof

Proof of the travel document's chip authenticity

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Chip Authentication Version 1 as defined in [5]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application Note 23 The **OT.Chip_Auth_Proof** implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [2] [3] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

5.1.13. OT.Active_Auth_Proof

Proof of the travel document's chip authenticity by Active Authentication

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [5]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

5.2. Security Objectives for the Operational Environment

This section introduces the security objectives to be achieved by the environment.

Travel document Issuer as the general responsible

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

5.2.1. OE.Legislative_Compliance

Issuing of the travel document

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 20):

5.2.2. OE.Passive_Auth_Sign

Authentication of travel document by Signature

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [2] [3]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [2] [3]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

5.2.3. OE.Personalization

Personalization of travel document
The travel document Issuer must ensure that the Personalization Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalization) and store them in the travel document (electronic personalization) for the travel document holder as defined in [2] [3], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [2] [3] (in the role of a DS).

Terminal operator: Terminal's receiving branch

5.2.4. OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [2] [3].

2.) The related terminals implement the terminal parts of the PACE protocol [3], of the Passive Authentication [3] (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3.) The related terminals need not to use any own credentials.

4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [2] [3]).

5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Travel document holder Obligations

5.2.5. OE.Travel_Document_Holder

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

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

5.2.6. OE.Auth_Key_Travel_Document

Travel document Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to counter the Threat **T.Counterfeit** as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in the EAC PP [9] and not in [8].

5.2.7. OE.Active_Auth_Key_Document

Travel document 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 travel document by certification of the Active Authentication Public Key by means of the Document Security Object.

5.2.8. OE.Authoriz_Sens_Data

Authorization for Use of Sensitive Biometric Reference Data

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

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat **T.Read_Sensitive_Data**, the Organizational Security Policy **P.Sensitive_Data** and the Assumption **A.Auth_PKI** as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in the EAC PP [9] and not in [8].

Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives of the TOE environment.

5.2.9. OE.Exam_Travel_Document

Examination of the physical part of the travel document

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [3] and/or the Basic Access Control. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat **T.Counterfeit** and the Assumption **A.Insp_Sys** by demanding the Inspection System to perform the Chip Authentication protocol v.1. **OE.Exam_Travel_Document** also repeats partly the requirements from **OE.Terminal** in [8] and therefore also counters **T.Forgery** and **A.Passive_Auth** from [8]. This is done because a new type of Inspection System is introduced in the EAC PP [9] as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

5.2.10. OE.Prot_Logical_Travel_Document

Protection of data from the logical travel document

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Assumption **A.Insp_Sys** by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

5.2.11. OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

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

Justification: This security objective for the operational environment is needed additionally to those from [8] in order to handle the Threat **T.Read_Sensitive_Data**, the Organizational Security Policy **P.Sensitive_Data** and the Assumption **A.Auth_PKI** as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

5.3. Security Objective Rationale

The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and *necessity* of the objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all assumptions are addressed by the security objectives for the TOE environment.
Threats, assumptions and security objectives taken from the claimed PACE PP [8] are marked in *italics*. Other threats, assumptions and security objectives are taken from the claimed EAC PP [9] or defined in the current ST.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Identification*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*	OE.Auth_Key_Travel_Document	OE.Active_Auth_Key_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	*OE.Personalization*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*
T.Read_Sensitive_Data	X															X			X					
T.Counterfeit		X	X											X	X		X							
T.Skimming					X	X	X																X	
T.Eavesdropping							X																	
T.Tracing								X															X	
T.Abuse-Func									X															
T.Information_Leakage										X														
T.Phys-Tamper												X												
T.Malfunction													X											
T.Forgery				X	X	X			X			X					X			X	X	X		
P.Sensitive_Data	X															X			X					
P.Personalization				X							X									X				
P.Manufact											X													
P.Pre-Operational				X							X									X				X
P.Terminal																	X					X		
P.Card_PKI																					X			

P.Trustworthy_PKI																				X			
A.Insp_Sys																X	X						
A.Auth_PKI															X			X					
A.Passive_Auth																X				X			

A detailed justification required for *suitability* of the security objectives to coup with the security problem definition is given below.

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contactless interface. This threat is countered by the security objectives **OT.Data_Integrity, OT.Data_Authenticity** and **OT.Data_Confidentiality** through the PACE authentication. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the travel document holder itself or by an authorized person or device, and, hence, cannot be captured by an attacker.

The threat **T.Eavesdropping** addresses listening to the communication between the TOE and a rightful terminal in order to gain the User Data transferred there. This threat is countered by the security objective **OT.Data_Confidentiality** through a trusted channel based on the PACE authentication.

The threat **T.Tracing** addresses gathering TOE tracing data identifying it remotely by establishing or listening to a communication via the contactless interface of the TOE, whereby the attacker does not a priori know the correct values of the PACE password. This threat is directly countered by security objectives **OT.Tracing** (no gathering TOE tracing data) and **OE.Travel_Document_Holder** (the attacker does not a priori know the correct values of the shared passwords).

The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-coded security functionality. The security objective **OT.Prot_Abuse-Func** ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

The threats **T.Information_Leakage**, **T.Phys-Tamper** and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is obviously addressed by the directly related security objectives **OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper** and **OT.Prot_Malfunction**, respectively.

The threat **T.Forgery** addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. The security objective **OT.AC_Pers** requires the TOE to limit the write access for the travel document to the trustworthy Personalization Agent (cf. **OE.Personalization**). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives **OT.Data_Integrity** and **OT.Data_Authenticity**, respectively. The objectives **OT.Prot_Phys-Tamper** and **OT.Prot_Abuse-Func** contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to **OE.Terminal** and performing the Passive Authentication using the Document Security Object as aimed by **OE.Passive_Auth_Sign** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally to the security objectives from PACE PP [8] which

counter this threat, the examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

The threat **T.Counterfeit** “Counterfeit of travel document chip data” addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** “Proof of travel document’s chip authentication” using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** “Travel document Authentication Key”. According to **OE.Exam_Travel_Document** “Examination of the physical part of the travel document” the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document’s chip.

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

The OSP **P.Sensitive_Data** “Privacy of sensitive biometric reference data” is fulfilled and the threat **T.Read_Sensitive_Data** “Read the sensitive biometric reference data” is countered by the TOE-objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data” requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

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

The OSP **P.Manufact** “Manufacturing of the travel document’s chip” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by **OT.Identification**.

The OSP **P.Pre-Operational** is enforced by the following security objectives: **OT.Identification** is affine to the OSP’s property ‘traceability before the operational phase’; **OT.AC_Pers** and **OE.Personalization** together enforce the OSP’s properties ‘correctness of the User- and the TSF-data stored’ and ‘authorisation of

Personalization Agents'; **OE.Legislative_Compliance** is affine to the OSP's property 'compliance with laws and regulations'.

The OSP **P.Terminal** is obviously enforced by the objective **OE.Terminal**, whereby the one-to-one mapping between the related properties is applicable. Additionally, this OSP is countered by the security objective **OE.Exam_Travel_Document. OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

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

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

The examination of the travel document addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** "Protection of data from the logical travel document" require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

The assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** "Authentication of travel document by Signature" from PACE PP [8] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_Travel_Document** "Examination of the physical part of the travel document".

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

6. Extended Components Definition

This security target uses components defined as extensions to CC part 2 [20]. These components are drawn from the PACE PP [8] and the EAC PP [9].

6.1. Definition of the Family FIA_API

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

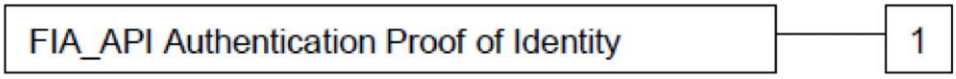
Application Note 24 The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1
The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit:There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

6.2. Definition of the Family FAU_SAS

To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

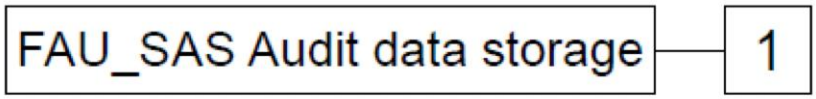
The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

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

Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

6.3. Definition of the Family FCS_RND

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

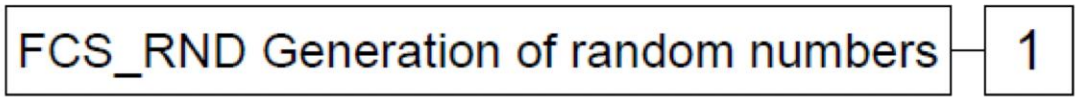
The family 'Generation of random numbers (FCS_RND)' is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

6.4. Definition of the Family FMT_LIM

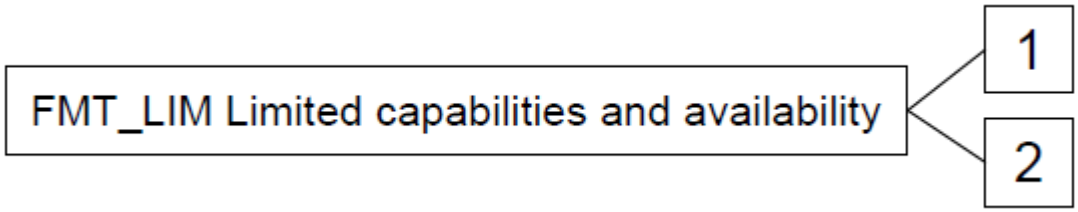
The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: *Limited capability and availability policy*].

FMT_LIM.2 Limited availability

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: *Limited capability and availability policy*].

Application Note 25 The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that:

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

or conversely

(ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

6.5. Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [20].

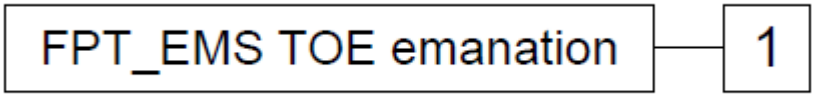
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1
There are no actions defined to be auditable.

FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

7. Security Functional Requirements for the TOE

The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment* and *iteration* are defined in sec. 8.1 of Part 1 [19] of the CC. 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. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are ~~crossed out~~.

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 authors are denoted as underlined text. Selections that have been made by the ST author are denoted as **bold 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 authors are denoted by showing as underlined text. Assignments that have been made by the ST author are denoted as **bold 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.
For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

7.1. TOE Security Functional Requirements

7.1.1. Class FCS Cryptographic Support

7.1.1.1. Cryptographic key generation (FCS_CKM.1)

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] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to** [18] and specified cryptographic key sizes **112, 128, 192, 256 bit** that meet the following: [3].

Application Note 26 The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [3]. This protocol is based on the ECDH compliant to TR-03111 [18] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [3] and [18] for details). The shared secret value *K* is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-

KMAC, PACE-KENC) according to [3] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application Note 27 FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [3].

Application Note 28 Triple-DES algorithm with 112 bit key size is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. The hash function SHA-1 is required for key derivation, which is also deprecated according to SOG-IS ACM [15]. Triple-DES and SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.

Application Note 29

The following elliptic curves are supported in PACE with ECDH:

- NIST P-224 (secp224r1)
- NIST P-256 (secp256r1)
- NIST P-384 (secp384r1)
- NIST P-521 (secp521r1)
- BrainpoolP224r1
- BrainpoolP256r1
- BrainpoolP320r1
- BrainpoolP384r1
- BrainpoolP512r1

The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. These curves are included in the evaluation scope for compatibility with ePassport application standards.

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 **3DES, AES key derivation** and specified cryptographic key sizes **112, 128, 192, 256 bit** that meet the following: **based on an ECDH protocol compliant to** [18]

Application Note 30 FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [5].

Application Note 31 The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [5]. This protocol is based on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [18], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [3]).

Application Note 32 The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 ([5]). The TOE may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [5] for details).

Application Note 33 Triple-DES algorithm with 112 bit key size is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. The hash function SHA-1 is required for key derivation, which is also deprecated according to SOG-IS ACM [15]. Triple-DES and SHA-1 are included in the evaluation scope for compatibility with ePassport application standards.

Application Note 34

The following elliptic curves are supported in CA with ECDH:

- NIST P-224 (secp224r1)
- NIST P-256 (secp256r1)
- NIST P-384 (secp384r1)
- NIST P-521 (secp521r1)
- BrainpoolP224r1
- BrainpoolP256r1
- BrainpoolP320r1
- BrainpoolP384r1
- BrainpoolP512r1

The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. These curves are included in the evaluation scope for compatibility with ePassport application standards.

FCS_CKM.1/SCP Cryptographic key generation – SCP 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/SCP	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **AES key derivation** and specified cryptographic key sizes **128, 192, 256 bit** that meet the following:**GPC_SPE_014** [23].

Application Note 35 The TOE supports AES with 128, 192, 256 bit key size (SCP03).

7.1.1.2. Cryptographic key destruction (FCS_CKM.4)

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]

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

Application Note 36 The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. 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.

Application Note 37 The TOE shall destroy any session keys in accordance with FCS_CKM.4 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.

7.1.1.3. Cryptographic operation (FCS_COP.1)

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption/Decryption AES/TDES

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

Application Note 38

- 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-KEnc).
- The TOE supports Triple-DES with 112 bit key size and AES with 128, 192, 256 bit key size for PACE protocol.
- Triple-DES algorithm with 112 bit key size is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. It is in the evaluation scope for compatibility with ePassport application standards.

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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **CMAC, Retail-MAC** and cryptographic key sizes **112, 128, 192, 256** bit that meet the following: compliant to [3].

Application Note 39 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-KMAC). Note that in accordance with [3] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

Application Note 40 The Retail MAC algorithm is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. It is included in the evaluation scope for compatibility with ePassport application standards.

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, 3DES in CBC mode** and cryptographic key sizes **112, 128, 192, 256 bit** that meet the following: **compliant to** [3]**.**

Application Note 41

- 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.
- Triple-DES algorithm with 112 bit key size is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. It is in the evaluation scope for compatibility with ePassport application standards.

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, Retail-MAC** and cryptographic key sizes **112, 128, 192, 256 bit** that meet the following: **compliant to** [3]**.**

Application Note 42 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.

Application Note 43 The Retail MAC algorithm is already deprecated according to specified limit date (31st December 2024) mentioned on SOG-IS ACM [15]. It is included in the evaluation scope for compatibility with ePassport application standards.

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-224, SHA-256, SHA-384, SHA-512** and cryptographic key sizes **224, 256, 320, 384, 512 bit** that meet the following: **ISO15946-2** [24].

Application Note 44

- The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.
- The hash function SHA-224 is identified as legacy by SOG-IS ACM [15], which current expiration date is until 31st December 2025. It is included in the evaluation scope for compatibility with ePassport application standards.
- The following elliptic curves are supported in TA with ECDSA:
  - NIST P-224 (secp224r1)
  - NIST P-256 (secp256r1)
  - NIST P-384 (secp384r1)
  - BrainpoolP224r1
  - BrainpoolP256r1
  - BrainpoolP320r1
  - BrainpoolP384r1

- BrainpoolP512r1

The underlined elliptic curves above are not agreed by SOG-IS ACM [15]. These curves are included in the evaluation scope for compatibility with ePassport application standards.

FCS_COP.1/AA_SIGN Cryptographic operation – Signature for Active 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/ AA_SIGN	The TSF shall perform **digital signature creation for Active Authentication Data** in accordance with a specified cryptographic algorithm **RSA CRT** and cryptographic key sizes **2048, 3096, 4096 bit** that meet the following: **ISO-9796-2 Digital Signature scheme 1** [16]**.**

Application Note 45 This SFR has been added by the ST author to specify the cryptographic algorithm and key sizes used by the TOE to perform an Active Authentication in accordance with ICAO Doc 9303-11.

Application Note 46 For RSA cryptography, the TOE makes use of the cryptographic library embedded in the chip.

Application Note 47 Following SOG-IS ACM [15], the RSA CRT algorithm with key sizes from 1900 bits to 2999 bits is legacy. The current expiration date for the legacy use of key sizes from 1900 bits to 2999 bits is until 31st December 2025. The RSA-CRT algorithm with key size 2048 bits is in the evaluation scope for compatibility with ePassport application standards. However, key size of 3096 and 4096 bits is recommended.

FCS_COP.1/SCP_ENC Cryptographic operation – SCP 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/SCP_ 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** that meet the following: **GPC_SPE_014** [23].

FCS_COP.1/SCP_MAC Cryptographic operation – SCP 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/SCP_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** that meet the following: **GPC_SPE_014** [23].

FCS_COP.1/SCP_KEY_DEC Cryptographic operation - SCP key data 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/ SCP_KEY_DEC	The TSF shall perform **on-card key sensitive data decryption** in accordance with a specified cryptographic algorithm **AES in CBC mode** and cryptographic key sizes **128, 192, 256 bit** that meet the following: **GPC_SPE_014** [23].

FCS_COP.1/SHA Cryptographic operation – Hash

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, SHA-256** and cryptographic key sizes **none** that meet the following: **FIPS 180-4**.

Application Note 48

- The hash function SHA-256 is used to derive 192, 256 bit AES key in PACE or CA protocol, and it is used for signature generation during Active Authentication protocol.
- The hash function SHA-1 is required to derive the 112 bit Triple-DES key and 128 bit AES key in PACE or CA protocol, which is deprecated according to SOG-IS ACM [15]. SHA-1 is included in the evaluation scope for compatibility with ePassport application standards.

7.1.1.4. Random Number Generation (FCS_RND.1)

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 **quality criteria defined in AIS-31 publication by the German BSI. In particular, it considers requirements for devices belonging to the functional class PTG.2 (strength of mechanism: high)**.

Application Note 49 This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

7.1.2. Class FIA Identification and Authentication

7.1.2.1. FIA_UID.1 Timing of identification

FIA_UID.1/PACE Timing of identification - PACE

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 [3],

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 [5]

5.to carry out the Terminal Authentication Protocol v.1 according to [5]

6.to carry out the Active Authentication Mechanism

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

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

Application Note 50 The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [8] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

Application Note 51 In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. The Inlay&MRTD Manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the travel document”. The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization Agent Key).

Application Note 52 User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorized other person or device (Basic Inspection System with PACE).

Application Note 53 In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialization Data and/or Pre-personalization Data in the audit records of the IC. Please note that a Personalization Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalization Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role ‘Personalization Agent’, when a terminal proves the respective Terminal Authorization Level as defined by the related policy (policies).

FIA_UID.1/SCP Timing of identification - SCP

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/SCP	The TSF shall allow **1.to establish a communication channel,** **2.carrying out the mutual authentication according to GPC_SPE_014** [23]**,** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/SCP	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.2.2. FIA_UAU.1 Timing of authentication

FIA_UAU.1/PACE Timing of authentication - PACE

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 [3], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to identify themselves by selection of the authentication key 5. to carry out the Chip Authentication Protocol Version 1 according to [5] 6. to carry out the Terminal Authentication Protocol Version 1 according to [5] **7. to carry out the Active Authentication Mechanism** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 54 The SFR FIA_UAU.1/PACE in the current ST covers the definition in PACE PP [8] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

Application Note 55 The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (BIS-PACE).If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-KMAC, PACE-KENC), cf. FTP_ITC.1/PACE.

FIA_UAU.1/SCP Timing of authentication - SCP

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1/SCP	The TSF shall allow **1. to establish a communication channel,** **2. carrying out the mutual authentication according to GPC_SPE_014** [23]**.** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/SCP	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.2.3. FIA_UAU.4 Single-use authentication mechanisms

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 [3],

2.Authentication Mechanism based on **AES**

3.Terminal Authentication Protocol v.1 according to [5].

Application Note 56 The SFR FIA_UAU.4.1 in the current ST covers the definition in PACE PP [8] 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 [8].

Application Note 57 The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalization Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

7.1.2.4. FIA_UAU.5 Multiple authentication mechanisms

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 [3],

2.Passive Authentication according to [3],

3.Secure messaging in MAC-ENC mode according to [3],

4.Symmetric Authentication Mechanism based on **AES**

5.Terminal Authentication Protocol v.1 according to [5],

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 Authentication Mechanism with Personalization Agent Key(s)**.

3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.

4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.

5. **None.**

Application Note 58 The SFR FIA_UAU.5.1/PACE in the current ST covers the definition in PACE PP [8] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in PACE PP [8] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

7.1.2.5. FIA_UAU.6 Re-authenticating

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.

Application Note 59 The PACE protocol specified in [3] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

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.

Application Note 60 The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [3] 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.

7.1.2.6. FIA_API.1 Authentication Proof of Identity

FIA_API.1/CA Authentication Proof of Identity – Chip Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CA The TSF shall provide a Chip Authentication Protocol Version 1 according to [5] to prove the identity of the TOE.

Application Note 61 This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [5]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (ECDH) and two session keys for secure messaging in ENC_MAC mode according to [3]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his

protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity – Active Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA The TSF shall provide a **Active Authentication Protocol according to ICAO Doc9303-11** to prove the identity of the **TOE**.

7.1.2.7. FIA_AFL.1 Authentication Failure handling

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PACE The TSF shall detect when **1** unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met, the TSF shall **consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords**.

Application Note 62 The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [3]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorization data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[5], the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack[6] requiring an attack potential beyond high, so that the threat **T.Tracing** can be averted in the frame of the security policy of the current ST. One of some

[5] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.
[6] guessing CAN or MRZ, see T.Skimming above

opportunities for performing this operation might be '*consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords*'.

7.1.3. Class FDP User Data Protection

7.1.3.1. FDP_ACC.1 Subset access control

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

Application Note 63 The SFR FDP_ACC.1/TRM in the current ST covers the definition in PACE PP [8] 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.

7.1.3.2. FDP_ACF.1 Security attribute based access control

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.Authorisation of the Terminal.

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [3] after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

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

1.Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.

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

3.Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

4.Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.

5.Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.

6.Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4

Application Note 64 The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACE PP [8] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACE PP. The SFR FDP_ACF.1.4/TRM in the current ST covers the definition in PACE PP and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.

Application Note 65 The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [5]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Application Note 66 Please note that the Document Security Object (SOD) stored in EF.SOD (see [2] and [3]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [3].

7.1.3.3. FDP_RIP.1 Subset residual information protection

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 - SKPICC- PACE (by having generated a DH shared secret *K*),

3. **None**.

Application Note 67 The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

7.1.3.4. FDP_UCT.1 Basic data exchange confidentiality

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]

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

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.

7.1.3.5. FDP_UIT.1 Data exchange integrity

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] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
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.

Application Note 68 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).

7.1.4. Class FTP Trusted Path/Channels

7.1.4.1. FTP_ITC.1 Inter-TSF trusted channel

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.

Application Note 69 The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

Application Note 70 The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-KMAC, PACE-KENC): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of *operational* trusted channel; the cryptographic primitives being used for the secure messaging are as required by

FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

Application Note 71 Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

7.1.5. Class FAU Security Audit

7.1.5.1. FAU_SAS.1 Audit storage

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 Initialisation and Pre-Personalization Data in the audit records.

Application Note 72 The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the Inlay&MRTD Manufacturer in the Manufacturer role write the Initialisation 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.

7.1.6. Class FMT Security Management

7.1.6.1. FMT_SMR.1 Security Roles

FMT_SMR.1/PACE Security Roles - PACE

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/PACE	The TSF shall maintain the roles 1.Manufacturer , 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.

Application Note 73 The SFR FMT_SMR.1.1/PACE in the current ST covers the definition in PACE PP [8] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

7.1.6.2. FMT_SMF.1 Specification of Management Functions

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.

7.1.6.3. FMT_LIM.1 Limited capabilities

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 does not allow, 1.User Data to be manipulated and disclosed, 2.TSF data to be disclosed or manipulated, 3.software to be reconstructed, 4.substantial information about construction of TSF to be gathered which may enable other attacks and 5.sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

7.1.6.4. FMT_LIM.2 Limited availability

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 does not allow: 1.User Data to be manipulated and disclosed, 2.TSF data to be disclosed or manipulated 3.software to be reconstructed, 4.substantial information about construction of TSF to be gathered which may enable other attacks and 5.sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

Application Note 74 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 to provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application Note 75 The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

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

7.1.6.5. FMT_MTD.1 Management of TSF data

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to write the 1.initial Country Verifying Certification Authority Public Key, 2.initial Country Verifying Certification Authority Certificate, 3.initial Current Date, **4. None** to **the Personalization Agent**.

Application Note 76 The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [5]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

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

Application Note 77 The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [5]). 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. [5]).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write the Initialisation Data and Pre-personalization Data to the Manufacturer.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to read out the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.

Application Note 78 The TOE may restrict the ability to write the Initialisation Data and the Pre-personalization Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases ‘manufacturing ’and ‘issuing’, but being not needed and may be misused in the ‘operational use’. Therefore, read and use access to the Initialisation Data shall be blocked in the ‘operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase ‘issuing 'to the life cycle phase ‘operational use’.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
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.

Application Note 79 The authorized roles are identified in their certificate (cf. [5]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [5]).

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

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

Application Note 80 The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read the 1.PACE passwords , 2.Chip Authentication Private Key, 3.Personalization Agent Keys **4.Active Authentication Private Key** to none.

Application Note 81 The SFR FMT_MTD.1/KEY_READ in the current ST covers the definition in PACE PP [8] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

FMT_MTD.1/PA Management of TSF data – Personalization agent

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1.1/PA	The TSF shall restrict the ability to write the Document Security Object (SOD) to the Personalization Agent.

Application Note 82 By writing SOD into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness and genuineness of all the personalization data related. This consists of user- and TSF- data.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/AAPK	The TSF shall restrict the ability to **write** the **Active Authentication Private Key** to **the Personalization Agent**.

Application Note 83 The addition of this SFR does not impair the conformance to the Protection Profiles.

7.1.6.6. FMT_MTD.3 Secure TSF data

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.

Application Note 84 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.

7.1.7. Class FPT Protection of the Security Functions

7.1.7.1. FPT_EMS.1 TOE Emanation

FPT_EMS.1 TOE Emanation	
Hierarchical to:	No other components.
Dependencies:	No dependencies
FPT_EMS.1.1	The TOE shall not emit **the shape and amplitude of signals, the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines during internal operations or data transmissions** in excess of **unintelligible limits** enabling access to 1.Chip Authentication Session Keys 2.PACE session Keys (PACE-KMAC, PACE-KENC), 3.the ephemeral private key ephem SKPICC-PACE, **4.none,** 5.Personalization Agent Key(s), 6.Chip Authentication Private Key and **7.Active Authentication Private Key.**

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-KMAC, PACE-KENC),

3.the ephemeral private key ephem SKPICC-PACE,

4.**none,**

5.Personalization Agent Key(s) and

6.Chip Authentication Private Key and

7.**Active Authentication Private Key**.

Refinement: The TSF shall ensure any user are unable to use the smart card circuits contacts to gain access to TSF data and User Data in any unintended mode violating the security policy defined by FDP_ACC.1/TRM, FDP_ACF.1/TRM, FMT_MTD.1/INI_DIS, and FMT_MTD.1/KEY_READ.

Application Note 85 The SFR FPT_EMS.1.1 in the current ST covers the definition in PACE PP [8] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in the current ST covers the definition in PACE PP and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

Application Note 86 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 travel document's chip provides a smart card contactless interface (the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

7.1.7.2. FPT_FLS.1 Failure with preservation of secure state

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.**

7.1.7.3. FPT_TST.1 TSF testing

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 authorised users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application Note 87 If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user 'Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

7.1.7.4. FPT_PHP.3 Resistance to physical attack

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.

Application Note 88 The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, ‘automatic response ’means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

8. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 5 (EAL5+)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

The table below summarizes the assurance components that define the security assurance requirements for the TOE.

Table 7 Assurance requirements at EAL5+

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_INT.2, ADV_TDS.4
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_COV.2, ATE_DPT.3, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.5

9. Security Requirements Rationale

9.1. Security Functional Requirements Rationale

The table below provides an overview for security functional requirements coverage of security objectives. SFRs and security objectives taken from the claimed PACE PP [8] are marked in *italics*. Other SFRs and security objectives are taken from the claimed EAC PP [9] or defined in the current security target.

Additions due to hash function, Active Authentication and SCP protocol are shaded.

Table 8 Coverage of TOE security objectives by SFRs

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*
FAU_SAS.1				X				X					
FCS_CKM.1/DH_PACE					X	X	X						
FCS_CKM.1/CA	X	X			X	X	X						
FCS_CKM.1/SCP				X	X	X	X						
FCS_CKM.4	X			X	X	X	X						
FCS_COP.1/PACE_ENC							X						
FCS_COP.1/CA_ENC	X	X			X		X						
FCS_COP.1/PACE_MAC					X	X							
FCS_COP.1/CA_MAC	X	X			X								
FCS_COP.1/SIG_VER	X												
FCS_COP.1/AA_SIGN			X			X							
FCS_COP.1/SCP_ENC				X			X						
FCS_COP.1/SCP_MAC				X	X	X							
FCS_COP.1/SCP_KEY_DEC				X			X						
FCS_COP.1/SHA		X	X		X	X	X						
FCS_RND.1	X			X	X	X	X						
FIA_AFL.1/PACE											X		
FIA_UID.1/PACE	X			X	X	X	X						
FIA_UID.1/SCP	X			X	X	X	X						
FIA_UAU.1/PACE	X			X	X	X	X						
FIA_UAU.1/SCP	X			X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*
FIA_UAU.5/PACE	X			X	X	X	X						
FIA_UAU.6/PACE					X	X	X						
FIA_UAU.6/EAC	X				X	X	X						
FIA_API.1/CA		X											
FIA_API.1/AA			X										
FDP_ACC.1/TRM	X			X	X		X						
FDP_ACF.1/TRM	X			X	X		X						
FDP_RIP.1					X	X	X						
FDP_UCT.1/TRM	X				X		X						
FDP_UIT.1/TRM					X		X						
FMT_SMF.1		X		X	X	X	X	X					
FMT_SMR.1/PACE		X		X	X	X	X	X					
FMT_LIM.1									X				
FMT_LIM.2									X				
FMT_MTD.1/INI_ENA				X				X					
FMT_MTD.1/INI_DIS				X				X					
FMT_MTD.1/CVCA_INI	X												
FMT_MTD.1/CVCA_UPD	X												
FMT_MTD.1/DATE	X												
FMT_MTD.1/CAPK	X	X			X								
FMT_MTD.1/PA				X	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X	X	X	X	X						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*
FMT_MTD.1/AAPK			X		X								
FMT_MTD.3	X												
FPT_EMS.1				X						X			
FPT_TST.1										X			X
FPT_FLS.1										X			X
FPT_PHP.3					X					X		X	
FTP_ITC.1/PACE					X	X	X				X		

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

The security objective **OT.AC_Pers** “Access Control for Personalization of logical travel document” addresses the access control of the writing the logical travel document. The justification for the SFRs **FAU_SAS.1**, **FMT_MTD.1/INI_ENA** and **FMT_MTD.1/INI_DIS** arises from the justification for **OT.Identification** above with respect to the Pre-personalization Data. The write access to the logical travel document data are defined by the SFR **FIA_UID.1/PACE**, **FIA_UAU.1/PACE**, **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM** in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. **FMT_MTD.1/PA** covers the related property of **OT.AC_Pers** (writing SOD and, in generally, personalization data). The SFR **FMT_SMR.1/PACE** lists the roles (including Personalization Agent) and the SFR **FMT_SMF.1** lists the TSF management functions (including Personalization). The SFRs **FMT_MTD.1/KEY_READ** and **FPT_EMS.1** restrict the access to the Personalization Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR **FIA_UAU.4/PACE** and **FIA_UAU.5/PACE**. The Personalization Terminal authenticates itself to the TOE based on GlobalPlatform SCP03 protocol by using the symmetric authentication mechanism with Personalization

Agent Key, the TOE will use TSF according to the **FCS_CKM.1/SCP** (for the generation of SCP03 session keys), **FIA_UID.1/SCP** and **FIA_UAU.1/SCP** (to establish the SCP03 secure channel), **FCS_RND.1** (for the generation of random challenge), **FCS_COP.1/SCP_KEY_DEC**, **FCS_COP.1/SCP_ENC** and **FCS_COP.1/SCP_MAC** (to ensure the confidentiality and integrity of the data transferred). The session keys are destroyed according to **FCS_CKM.4** after use.

The security objective **OT.Data_Integrity** "Integrity of personal data" requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by **FPT_PHP.3**. Logical manipulation of stored user data is addressed by (**FDP_ACC.1/TRM**, **FDP_ACF.1/TRM**): only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). **FMT_MTD.1/PA** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy. The Personalization Agent must identify and authenticate themselves according to **FIA_UID.1/PACE** and **FIA_UAU.1/PACE** before accessing these data. **FIA_UAU.4/PACE**, **FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the protocols used. The SFR **FMT_SMR.1/PACE** lists the roles and the SFR **FMT_SMF.1** lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by **FDP_UCT.1/TRM**, **FDP_UIT.1/TRM** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_MAC**. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (**FIA_UID.1/PACE, FIA_UAU.1/PACE**) using **FCS_COP.1/SHA** and **FCS_CKM.1/DH_PACE,** and possessing the special properties **FIA_UAU.5/PACE, FIA_UAU.6/PACE** resp. **FIA_UAU.6/EAC**. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. **FDP_RIP.1** requires erasing the values of session keys (here: for KMAC). The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords.

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

The SFR **FMT_MTD.1/CAPK, FMT_MTD.1/AAPK** and **FMT_MTD.1/KEY_READ** requires that the Chip Authentication Key and Active Authentication key cannot be written unauthorized or read afterwards. The SFR **FCS_RND.1** represents a general support for cryptographic operations needed.

For SCP03, the SFR **FCS_COP.1/SCP_MAC** ensures the integrity of the data transferred over a dedicated Secure Channel after authentication of the authorized user according to **FIA_UID.1/SCP, FIA_UAU.1/SCP** and **FCS_CKM.1/SCP**.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_MAC**. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1

(**FIA_UID.1/PACE, FIA_UAU.1/PACE**) using **FCS_COP.1/SHA, FCS_CKM.1/DH_PACE** resp. **FCS_CKM.1/CA** and possessing the special properties **FIA_UAU.5/PACE, FIA_UAU.6/PACE** resp. **FIA_UAU.6/EAC**. **FDP_RIP.1** requires erasing the values of session keys (here: for KMAC). **FIA_UAU.4/PACE, FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the protocols used. The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords and the Chip Authentication Private Key. **FMT_MTD.1/PA** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy. The SFR **FCS_RND.1** represents a general support for cryptographic operations needed. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related. The SFR **FCS_COP.1/AA_SIGN** and **FCS_COP.1/SHA** support the proof of chip authenticity using digital signature during Active Authentication.

For SCP03, the SFR **FCS_COP.1/SCP_MAC** ensures the authenticity of the data transferred over a dedicated Secure Channel after authentication of the authorized user according to **FIA_UID.1/SCP, FIA_UAU.1/SCP** and **FCS_CKM.1/SCP**.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (**FDP_ACC.1/TRM, FDP_ACF.1/TRM**). **FIA_UAU.4/PACE, FIA_UAU.5/PACE** and **FCS_CKM.4** represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by **FDP_UCT.1/TRM, FDP_UIT.1/TRM** and **FTP_ITC.1/PACE** using **FCS_COP.1/PACE_ENC** resp. **FCS_COP.1/CA_ENC**. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (**FIA_UID.1/PACE, FIA_UAU.1/PACE**) using **FCS_COP.1/SHA, FCS_CKM.1/DH_PACE** resp. **FCS_CKM.1/CA** and possessing the special properties **FIA_UAU.5/PACE, FIA_UAU.6/PACE** resp. **FIA_UAU.6/EAC**. **FDP_RIP.1** requires erasing the values of session keys (here: for KENC). The SFR **FMT_MTD.1/KEY_READ** restricts the access to the PACE passwords and the Chip Authentication Private Key. **FMT_MTD.1/PA** requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered trustworthy .The SFR **FCS_RND.1** represents the general support for cryptographic operations needed. The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.

For SCP03, the SFR **FCS_COP.1/SCP_ENC** ensures the confidentiality of the data transferred over a dedicated Secure Channel after authentication of the authorized user according to **FIA_UID.1/SCP, FIA_UAU.1/SCP, FCS_CKM.1/SCP** and **FCS_COP.1/SCP_KEY_DEC**.

The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM** allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according **FCS_COP.1/SIG_VER**.

The SFRs **FIA_UID.1/PACE** and **FIA_UAU.1/PACE** require the identification and authentication of the inspection systems. The SFR **FIA_UAU.5/PACE** requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by **FIA_UAU.4/PACE**. The SFR **FIA_UAU.6/EAC** and **FDP_UCT.1/TRM** requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to **FCS_RND.1** (for the

generation of the terminal authentication challenge), **FCS_CKM.1/CA** (for the generation of shared secret and for the derivation of the new session keys), and **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_MAC** for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to **FCS_CKM.4** after use. The SFR **FMT_MTD.1/CAPK** and **FMT_MTD.1/KEY_READ** requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

FIA_UID.1/SCP and **FIA_UAU.1/SCP** requires the identification and authentication based on Secure Channel SCP03.

The security objective **OT.Chip_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by **FIA_API.1/CA** proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by **FCS_CKM.1/CA** is performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/CAPK** and **FMT_MTD.1/KEY_READ**. The Chip Authentication Protocol v.1 [5] requires additional TSF according to **FCS_COP.1/SHA** and **FCS_CKM.1/CA** (for the derivation of the session keys), **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_MAC** (for the ENC_MAC_Mode secure messaging).The SFRs **FMT_SMF.1** and **FMT_SMR.1/PACE** support the functions and roles related.

The security objective **OT.Active_Auth_Proof** "Proof of travel Document's chip authenticity by Active Authentication" is ensured by the Active Authentication Mechanism [3] provided by **FIA_API.1/AA**, proving the identity of the TOE. The Active Authentication Protocol defined by **FIA_API.1/AA** is performed using a TOE internally stored confidential private key as required by **FMT_MTD.1/AAPK** and **FMT_MTD.1/KEY_READ**. This key is written to the TOE as defined by **FMT_MTD.1/AAPK**. The Active Authentication Protocol requires additional TSF according to **FCS_COP.1/SHA** and **FCS_COP.1/AA_SIGN** (for the digital signature creation of Active Authentication data).

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

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR **FPT_EMS.1**,

- by forcing a malfunction of the TOE which is addressed by the SFR **FPT_FLS.1** and **FPT_TST.1**, and/or

- by a physical manipulation of the TOE which is addressed by the SFR **FPT_PHP.3**.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication

via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows: (i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by **FIA_AFL.1/PACE**; (ii) for listening to PACE communication (is of importance for the current ST, since SOD is card-individual) – **FTP_ITC.1/PACE**.

The security objective **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” is covered by the SFR **FPT_PHP.3**.

The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by (i) the SFR **FPT_TST.1** which requires self-tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR **FPT_FLS.1** which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

9.2. Dependency Rationale

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. The following table shows the dependencies between the SFR of the TOE.

Table 9 **SFRs dependencies**

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	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. Fulfilled by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC Fulfilled by FCS_CKM.4
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC Fulfilled by FCS_CKM.4
FCS_CKM.1/SCP	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SCP_ENC, FCS_COP.1/SCP_MAC, FCS_COP.1/SCP_KEY_DEC Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/PACE_ENC	[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	Fulfilled by FCS_CKM.1/DH_PACE Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_MAC	[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	Fulfilled by FCS_CKM.1/DH_PACE Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/CA_ENC	[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	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[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	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4
FCS_COP.1/AA_SIGN	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	justification 3 for non-satisfied dependencies justification 2 for non-satisfied dependencies
FCS_COP.1/SCP_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/SCP Fulfilled by FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SCP_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/SCP Fulfilled by FCS_CKM.4
FCS_COP.1/SCP_KEY_DEC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/SCP Fulfilled by FCS_CKM.4
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	justification 4 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	N/A
FIA_UID.1/PACE	No dependencies	N/A
FIA_UID.1/SCP	No dependencies	N/A
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.1/SCP	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/SCP
FIA_UAU.4/PACE	No dependencies	N/A
FIA_UAU.5/PACE	No dependencies	N/A
FIA_UAU.6/PACE	No dependencies	N/A
FIA_UAU.6/EAC	No dependencies	N/A

SFR	Dependencies	Support of the Dependencies
FIA_API.1/CA	No dependencies	N/A
FIA_API.1/AA	No dependencies	N/A
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM justification 1 for non-satisfied dependencies
FDP_RIP.1	No dependencies	N/A
FDP_UCT.1/TRM	[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]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FDP_UIT.1/TRM	[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]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	N/A
FAU_SAS.1	No dependencies	N/A
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_SMF.1	No dependencies	N/A
FMT_LIM.1	FMT_LIM.2 Limited availability	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1 Limited capabilities	Fulfilled by FMT_LIM.1

SFR	Dependencies	Support of the Dependencies
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	N/A
FPT_FLS.1	No dependencies	N/A

SFR	Dependencies	Support of the Dependencies
FPT_TST.1	No dependencies	N/A
FPT_PHP.3	No dependencies	N/A

Rationale for non-satisfied dependencies

Justification 1: Dependency of FDP_ACF.1/TRM with FMT_MSA.3: The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

Justification 2: The SFR FCS_COP.1/AA_SIGN uses the asymmetric Key permanently stored during the Personalization process. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4.

Justification 3: The SFR FCS_COP.1/AA_SIGN uses the asymmetric Key loaded into TOE from outside during the Personalization process. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC.1/2. Since the TOE does not generate the key itself the FCS_CKM.1 is not applicable here.

Justification 4: The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

9.3. Security Assurance Requirements Rationale

EAL5+ is chosen for this TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL5 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks: the evaluators should have access to the low-level design and source code.

9.3.1. ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL5 is not enough. Due to the nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

9.3.2. AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 “Advanced methodical vulnerability analysis” is considered as the expected level for smart card products hosting sensitive applications, in particular in payment and identity areas. Moreover, this Security Target claims strict conformance to Protection Profiles [8] and [9], which includes AVA_VAN.5.

AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL5.

9.3.3. SARs dependencies in EAL5 + ALC_DVS.2 + AVA_VAN.5

Table 10 SARs dependencies

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

Requirements	CC Dependencies	Satisfied Dependencies
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

9.4. Security Requirements – 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 an internally consistent whole.

The dependency analysis in section 9.2 “Dependency rationale” 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-satisfied dependencies are appropriately explained.
All subjects and objects addressed by more than one SFR in section 7 “Security functional Requirements for the TOE” 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 class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 9.3 “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.
As this Security Target claims strict conformance to Protection Profiles [8] and [9], there is no inconsistence between functional and assurance requirements. Requirements dependencies are detailed in section 9.2 “Dependency rationale”. Furthermore, as discussed in section 9.3 “Security assurance requirements rationale”, the chosen assurance components are adequate for the functionality of the TOE.
Therefore, 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.

10. TOE Summary Specification

10.1. Implementation of SFRs in the TOE

The following table provides a general understanding of how the TOE is implemented by describing how the TOE meets each SFR.

Table 11 Implementation of SFRs in the TOE

Security Functional Requirement	Implementation
FCS_CKM.1/DH_PACE	The TOE generates session keys for Secure Messaging soon after a successful PACE authentication of the inspection terminal. The TOE supports PACE with ECDH and generates the AES or Triple-DES session keys.
FCS_CKM.1/CA	The TOE generates session keys for Secure Messaging soon after a successful Chip Authentication v1 of the inspection terminal. The TOE supports CA with ECDH and generates the AES or Triple-DES session keys.
FCS_CKM.1/SCP	For the authentication of the Personalization Agent, the TOE supports to perform mutual authentication by using the GlobalPlatform SCP03 protocol. The TOE generates AES session keys every time a secure channel is initiated based on SCP03.
FCS_CKM.4	Session keys are overwritten with zeros when a Secure Messaging session is closed.
FCS_COP.1/PACE_ENC	During a Secure Messaging session after a PACE authentication, the TOE encrypts transmitted data to ensure confidentiality, and decrypts received data, to restore original content. To this end, the TOE uses 2-Key Triple-DES in CBC mode with 112 bit key or AES with 128, 192 or 256 bit key.
FCS_COP.1/PACE_MAC	During a Secure Messaging session after a PACE authentication, the TOE computes a Message Authentication Code (MAC) to check integrity of received data, and to allow integrity check by the terminal. The MAC computation is performed according to 2-Key Triple-DES (112 bit) in Retail mode, or CMAC-AES algorithm with key sizes 128, 192 or 256 bits.
FCS_COP.1/CA_ENC	During a Secure Messaging session after a Chip Authentication v1, the TOE encrypts transmitted data to ensure confidentiality, and decrypts received data, to restore original content. To this end, the TOE uses Triple-DES in CBC mode with 112 bit key or AES with 128, 192 or 256 bit key.
FCS_COP.1/CA_MAC	During a Secure Messaging session after a Chip Authentication v1, the TOE computes a Message Authentication Code (MAC) to check integrity of received data, and to allow integrity check by the terminal. The MAC computation is performed according to 2-Key Triple-DES (112 bit) in Retail mode, or CMAC-AES algorithm with key sizes 128, 192 or 256 bits.
FCS_COP.1/SIG_VER	The TOE performs signature verification for Terminal Authentication using ECDSA algorithm with SHA-224, SHA-256, SHA-384, and SHA-512.

Security Functional Requirement	Implementation
FCS_COP.1/AA_SIGN	The TOE performs digital signature creation for Active Authentication using the RSA CRT cryptography with key size of 2048, 3096, 4096 bit.
FCS_COP.1/SCP_ENC	The TOE supports the mutual authentication by means of GP SCP03 protocol. To ensure data confidentiality, the TOE uses AES in CBC mode with 128, 192 or 256 bit keys to encrypt and decrypt the transmitted data.
FCS_COP.1/SCP_MAC	The TOE supports the mutual authentication by means of GP SCP03 protocol. To ensure data integrity and originality, the TOE uses CMAC for MAC calculation of the transmitted data.
FCS_COP.1/SCP_KEY_DEC	The TOE supports the mutual authentication by means of GP SCP03 protocol. The TOE uses AES-CBC mode with 128, 192 or 256 bit keys for key sensitive data decryption.
FCS_COP.1/SHA	The TOE implements hashing algorithm SHA-1 to be used for key derivation when 112 bit 3DES key or 128 bit AES key is used in PACE or CA protocol. The TOE implements hashing algorithm SHA-256 to be used for key derivation when 192, 256 bit AES key is used in PACE or CA protocol, and for signature generation during AA protocol.
FCS_RND.1	The TOE generates random numbers to be used during authentication protocols according to AIS31 class PTG.2 [25].
FIA_UID.1/PACE	The TOE applies access control policies to guarantee that the following actions can be performed before the user is identified: • Establishment of a secure communication channel, • PACE authentication • Read access to the initialization data • Chip Authentication (as CA v1 or as part of PACE-CAM), • Terminal Authentication, • Active Authentication. In phase 4 Operational use, the inspection system is allowed to access less sensitive data stored in the TOE after the successful run of PACE protocol. Sensitive data must only be accessible to the authorized inspection system by means of Extended Access Control (CA + TA). Active authentication can be used to verify the identity of chip.

Security Functional Requirement	Implementation
FIA_UID.1/SCP	The TOE applies access control policies to guarantee that the following actions can be performed before the user is identified: • Establishment of a secure communication channel, • Mutual Authentication based on SCP03. In phase 3 Personalization, GlobalPlatform SCP03 protocol is used for the identification and authentication of the Personalization Agent with the personalization agent key.
FIA_UAU.1/PACE	The TOE applies access control policies to guarantee that the following actions can be performed before the user is authenticated: • Establishment of a secure communication channel, • PACE authentication • Read access to the initialization data • Chip Authentication (as CA v1 or as part of PACE-CAM), • Terminal Authentication, • Active Authentication. In phase 4 Operational use, the inspection system is allowed to access less sensitive data stored in the TOE after the successful run of PACE protocol. Sensitive data must only be available to the authorized inspection system by means of Extended Access Control (CA + TA). Active authentication can be used to verify the identity of chip.
FIA_UAU.1/SCP	The TOE applies access control policies to guarantee that the following actions can be performed before the user is authenticated: • Establishment of a secure communication channel, • Mutual Authentication based on SCP03. In phase 3 Personalization, GlobalPlatform SCP03 protocol is used for the identification and authentication of the Personalization Agent with the personalization agent key.
FIA_UAU.4/PACE	The TOE generates the random challenge or nonce used for the authentication mechanisms by a random number generator of class PTG.2. The reuse of these authentication data is forbidden.

Security Functional Requirement	Implementation
FIA_UAU.5/PACE	The TOE provides: • the PACE mechanism to authenticate the user in the operational use, • the symmetric authentication mechanism (SCP03 protocol) to authenticate the Personalization agent, • Passive authentication to verify integrity of logical user data, • Secure Messaging in MAC-ENC mode, to guarantee confidentiality and integrity of data exchanged over a communication channel, • Terminal Authentication as final part of the EAC v1 mechanism to verify the user's access rights to the sensitive personal data.
FIA_UAU.6/PACE	Secure Messaging established after a successful PACE authentication allows re-authentication of the user. The TOE verifies the MAC of each command received from the PACE terminal.
FIA_UAU.6/EAC	Secure Messaging established after a successful Chip Authentication v1 provides re-authentication of the user. The TOE verifies the MAC of each command received from the inspection system.
FIA_API.1/CA	The TOE proves the genuineness of the chip by performing Chip Authentication v1. Other methods to achieve that proof are related to Active Authentication (FIA_API.1/AA).
FIA_API.1/AA	The TOE proves the genuineness of the chip by performing Active Authentication. Other methods to achieve that proof are related to Chip Authentication (FIA_API.1/CA).
FIA_AFL.1/PACE	In case of failed authentication attempt with PACE passwords during the PACE protocol, the TOE will consecutively prolong the waiting time for the next authentication attempts.
FDP_ACC.1/TRM	The TOE applies an Access Control Policy to check that terminals wanting to access protected data possess the required privileges and have successfully completed the required authentication. The TSF checks the possess of the above requirements before any access to protected data.

Security Functional Requirement	Implementation
FDP_ACF.1/TRM	The TOE keeps a security status for each of the data object related to the protected data listed in this SFR to guarantee entitlement to read and/or write those data. The TSF checks the security status is checked before any access to the protected data. In the operational use phase, only the PACE authenticated BIS-PACE can read the less sensitive user data stored in the TOE. The authenticated Extended Inspection System can read the sensitive personal data (EF.DG3, EF.DG4) from TOE based on the authorization of the terminal. The secret keys stored in TOE are not allowed to be read out by any user.
FDP_RIP.1	The TOE clears session keys and ephemeral private keys by overwriting them with zeros. The TOE also clears the context under which those keys have been used.
FDP_UCT.1/TRM	The TOE protects data confidentiality of received and transmitted data by means of Triple-DES or AES cryptography within Secure Messaging sessions in MAC-ENC mode, which is established after successful PACE or Chip Authentication.
FDP_UIT.1/TRM	The TOE guarantees data integrity by means of a Message Authentication Code (MAC) within Secure Messaging sessions in MAC-ENC mode, which is established after successful PACE or Chip Authentication. The MAC is computed on data to be transmitted and sent by TOE to the terminal together with the data and is checked upon data reception to allow tampering detection. The TOE also checks the MAC of data received from the terminal to verify the integrity.
FTP_ITC.1/PACE	After successful performing the PACE, the TOE establishes a secure channel with the terminal (the trusted IT product). After that, all data are exchanged in Secure Messaging in ENC_MAC mode. Therefore, confidentiality is protected by encryption and checking of MAC allows tampering detection.
FAU_SAS.1	The Manufacturer stores the Initialisation data and Pre-personalization data in the audit records.
FMT_SMR.1/PACE	The TOE distinguishes between the roles Manufacturer, Personalization Agent, Terminal, PACE-authenticated Basic Inspection System, CVCA, Document Verifier, Domestic and Foreign Extended Inspection System. All these roles are granted the access privileges allowed by the security policies and are implicitly identified via the corresponding authentication key.
FMT_SMF.1	The TOE provides features for storing Initialization data, Pre-personalization data, Personalization data and Configuration data, ensuring that only the entitled agents are able to do so.

Security Functional Requirement	Implementation
FMT_LIM.1	The test features of the OS, as well as the authentication mechanism granting access to them, are permanently disabled in the evaluated configuration of the OS. As regards the test features of the IC, information on their limitation is provided in the TOE summary specification of the public security target of the supported IC for platform SFRs FMT_LIM.1, FMT_LIM.2 [26].
FMT_LIM.2	The same as in FMT_LIM.1
FMT_MTD.1/CVCA_INI	CVCA public key and certificate, as well as current date can be written by the Personalization Agent only. The Personalization Agent must be successfully authenticated before the execution of this action.
FMT_MTD.1/CVCA_UPD	CVCA public key and certificate can be updated by the CVCA only. The TSF checks the possess of access privileges before any access is made to those data.
FMT_MTD.1/INI_ENA	In the manufacturing phase, only the entitled manufacturers can write the initialisation data and pre-personalization data into TOE. The TSF checks the access privileges before any access is made.
FMT_MTD.1/INI_DIS	Only the Personalization Agent can block the read access to the initialization data and Pre-personalisation data. The Personalization Agent must be successfully authenticated before the execution of this action. The initialization data and Pre-personalisation data is not allowed to be read out by the users in the operational use phase.
FMT_MTD.1/DATE	The current date can be updated by the CVCA, or DV or Domestic EIS only according to the authorization in their certificates.
FMT_MTD.1/CAPK	The Chip Authentication private key can be loaded by the Personalization Agent only. The Personalization Agent must be successfully authenticated before the execution of this action.
FMT_MTD.1/AAPK	The Active Authentication private key can be written by the Personalization Agent only. The Personalization Agent must be successfully authenticated before the execution of this action.

Security Functional Requirement	Implementation
FMT_MTD.1/KEY_READ	The property defining read access conditions of: • PACE passwords, • Chip Authentication private key, • Personalization agent keys, • Active Authentication private key are set, when those keys are written, so that the keys cannot be read by anyone under any circumstances. The TSF checks the access privileges before any access is made to those keys.
FMT_MTD.1/PA	The Document Security Object SO_D can only be written by the Personalization Agent. The Personalization Agent must be successfully authenticated before the execution of this action.
FMT_MTD.3	The TSF checks the security and the validity of values in the certificate chain before using those data for Terminal Authentication and Access Control mechanisms.
FPT_EMS.1	Leakage of confidential data through side channels is prevented by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [27].
FPT_FLS.1	In case self-test fails or a physical attack is detected, the OS enters an endless loop, so that all cryptographic operations and data output interfaces are inhibited.
FPT_TST.1	During initial start-up, the IC performs a self-test procedure that tests alarm lines and environmental sensor mechanisms (IC refs [26] [28]), and the OS checks the integrity of the TSF by computing a hash value of the code and comparing it with a reference hash value stored internally. Moreover, the integrity of TSF data is checked whenever they are used. In case any one of such checks fails, the OS enters an endless loop, so that the resulting fall of communication informs the user about the integrity error.
FPT_PHP.3	Detection of physical attacks is ensured by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [27].

10.2. Assurance Measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [21].

The implementation is based on a description of the security architecture of the TOE and on a semi-formal high-level and low-level design of the components of the TOE. The description is sufficient to generate the

TOE without other design requirements. These documents, together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

The configuration management plan addresses the ALC_CMC and ALC_CMS families and enforces good practices to securely manage configuration items including, but not limiting to, design documentation, user documentation, source code, test documentation and test data.
The configuration management process guarantees the separation of the development configuration libraries from the configuration library containing the releases and also supports the generation of the TOE.
All the configuration items are managed with the help of automated tools. In particular configuration items regarding security flaws are managed with the support of an issue tracking system, while all the other configuration items are managed with the help of a version control system.

The software test process, addressing the class ATE, is machine-assisted to guarantee a repeatable error-free execution of the same test chains in both the system test and in the validation phases.

A secure delivery of the TOE is guaranteed by the application of dedicated procedures. The prevention measures, the checks and all the actions to be performed at the developer's site are described in the secure delivery procedure addressing the family ALC_DEL, while the security measures related to delivery to be applied at the user's site are defined in the pre-personalization guidance. The latter document also addresses the family AGD_PRE.
The necessary information for the document personalization is provided by a dedicated guidance and the information for its usage after delivery to the legitimate holder is provided by the guidance for the operational use. These documents address the AGD_OPE assurance family.

To protect the confidentiality and integrity of the TOE design and implementation, the development and production environment and tools conform to the security policies defined in the documentation dedicated to the development security, which addresses the family ALC_DVS.
The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in dedicated documents addressing the families ALC_LCD and ALC_TAT.
An independent vulnerability analysis, meeting requirements of the family AVA_VAN, is conducted by a third party. Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the platform (IC) are covered by documents from the IC manufacturer [26] [28]. The security procedures described in such documents have been taken into consideration.

Table 12 Security Assurance Requirements for the current TOE

Security Assurance Requirements	Documentation
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 and automation
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery Procedures
ALC_DVS.2	Sufficiency of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.2	Compliance with implementation standards
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security Problem Definition
ASE_TSS.1	TOE summary specification
ATE_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

The assurance measures described in this section cover the assurance requirements in section 9.3.

11. Statement of Compatibility

This section provides an analysis of the compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) [26].

The following sections identify the parts of the Platform-ST that are relevant for the composite TOE. Subsequent sections aim to demonstrate the compatibility of each of those parts of the Platform-ST with their counterpart of the Composite-ST (the document at hand).

11.1. Relevance of the parts of the Platform-ST

The parts of the Platform-ST taken into account for the relevance evaluation are:

- Security Functional Requirements (SFRs)
- Security Objectives for the TOE
- Security Objectives for the operational environment

In the Platform-ST, some SFRs are defined inside the ST itself, and for the remaining SFRs the Platform-ST relies on the definition given in the IC Protection Profile BSI-CC-PP-0084-2014 [29].

The following table shows the mapping between the SFRs for the composite product (defined in the current ST) with the SFRs defined in the platform-ST [26]. In those cases where a matching exists, the platform-SFR is considered as relevant (RP_SFR); otherwise, the platform-SFR is considered as not relevant (IP_SFR).

The irrelevant platform-SFRs (**IP_SFR**) are listed as below:

FDP_SDC.1, FDP_SDI.2, FCS_RNG.1/HPRG, FCS_RNG.1/DRNG, FCS_RNG.1/DRNG4, FCS_RNG.1/RCL/TRNG, FCS_RNG.1/RCL/DRNG3, FCS_RNG.1/RCL/DRNG4, FMT_LIM.1/Loader, FMT_LIM.2/Loader, FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FCS_COP.1/RSA/ENC_v3.02.000, FCS_COP.1/RSA/ENC_v3.33.003_v3.34.000_v3.35.001, FCS_COP.1/RSA/DEC, FCS_COP.1/RSA/DEC_CRT, FCS_COP.1/RSA/SIG, FCS_COP.1/RSA/RSA_DH, FCS_COP.1/RSA/VER, FCS_CKM.1/ECC, FCS_CKM.1/RSA/<iteration>, FCS_CKM.4/RSA, FCS_CKM.4/ECC, FCS_COP.1/HCL, FCS_COP.1/ECC/SIG, FMT_MTD.1/Loader, FMT_SMR.1/Loader, FMT_SMF.1/Loader, FIA_UID.2/Loader, FPT_FLS.1/Loader, FIA_API.1

The relevant Platform-ST SFRs are categorized to two groups:

- **RP_SFR-SERV**: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
- **RP_SFR-MECH:** Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

Table 13 Relevance of the Platform-ST SFRs (defined in the Platform-ST [26])

Platform-ST SFRs (defined in the Platform-ST [26])	Composite-ST SFRs	Category
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES FCS_COP.1/ECC/DH FCS_COP.1/ECC/PACE_IM_ECDH	FCS_CKM.1/DH_PACE	RP_SFR-SERV
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES FCS_COP.1/ECC/DH	FCS_CKM.1/CA	RP_SFR-SERV
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_CKM.1/SCP	RP_SFR-SERV
FCS_CKM.4/SCP FCS_CKM.4/SCL	FCS_CKM.4	RP_SFR-SERV
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES	FCS_COP.1/PACE_ENC	RP_SFR-SERV
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES	FCS_COP.1/CA_ENC	RP_SFR-SERV
FCS_COP.1/SCL/TDES-MAC FCS_COP.1/SCL/AES-MAC	FCS_COP.1/PACE_MAC	RP_SFR-SERV
FCS_COP.1/SCL/TDES-MAC FCS_COP.1/SCL/AES-MAC	FCS_COP.1/CA_MAC	RP_SFR-SERV
FCS_COP.1/ECC/VER	FCS_COP.1/SIG_VER	RP_SFR-SERV
FCS_COP.1/RSA/SIG_CRT	FCS_COP.1/AA_SIGN	RP_SFR-SERV
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/SCP_ENC	RP_SFR-SERV
FCS_COP.1/SCL/AES-MAC	FCS_COP.1/SCP_MAC	RP_SFR-SERV
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/SCP_KEY_DEC	RP_SFR-SERV
FCS_RNG.1/TRNG	FCS_RND.1	RP_SFR-SERV

Platform-ST SFRs (defined in the Platform-ST [26])	Composite-ST SFRs	Category
FCS_RNG.1/TRNG	FIA_UAU.4/PACE	RP_SFR-SERV
FAU_SAS.1	FAU_SAS.1	RP_SFR-SERV
FMT_LIM.1 FMT_LIM.2	FMT_LIM.1	RP_SFR-SERV
FMT_LIM.1 FMT_LIM.2	FMT_LIM.2	RP_SFR-SERV
FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	FPT_EMS.1	RP_SFR-MECH
FRU_FLT.2 FPT_FLS.1	FPT_FLS.1	RP_SFR-MECH
FRU_FLT.2 FPT_FLS.1 FPT_TST.2	FPT_TST.1	RP_SFR-MECH
FPT_PHP.3	FPT_PHP.3	RP_SFR-MECH

The following table shows the mapping between the relevant platform-SFRs (analyzed above) with the platform-ST security objectives [26]. In those cases where a matching exists, the platform-ST security objective is considered as relevant; otherwise, the platform-ST security objective is considered as not relevant and not listed.

Table 14 Relevance of the Platform-ST security objectives for the TOE (defined in the Platform-ST [26])

Relevant Platform-ST SFRs	Platform-ST Security objectives for the TOE (defined in the Platform-ST [26])
FAU_SAS.1	O.Identification
FCS_CKM.4/SCP	O.TDES
FCS_CKM.4/SCL	O.TDES O.AES-TDES-MAC
FCS_COP.1/ECC/DH	O.ECC
FCS_COP.1/ECC/PACE_IM_ECDH	O.ECC
FCS_COP.1/SCP/TDES	O.TDES
FCS_COP.1/SCL/TDES	O.AES-TDES-MAC O.TDES
FCS_COP.1/SCP/AES	O.AES
FCS_COP.1/SCL/AES	O.AES-TDES-MAC O.AES
FCS_COP.1/SCL/TDES-MAC	O.AES-TDES-MAC
FCS_COP.1/SCL/AES-MAC	O.AES-TDES-MAC
FCS_COP.1/ECC/VER	O.ECC
FCS_COP.1/RSA/SIG_CRT	O.RSA

FCS_RNG.1/TRNG	O.RND
FMT_LIM.1	O.Abuse-Func
FMT_LIM.2	O.Abuse-Func
FDP_ITT.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FDP_IFC.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FPT_ITT.1	O.Leak-Inherent O.Leak-Forced O.Abuse-Func O.RND
FRU_FLT.2	O.Malfunction O.Leak-Forced O.Abuse-Func O.RND
FPT_FLS.1	O.Malfunction O.Leak-Forced O.Abuse-Func O.RND
FPT_TST.2	O.Phys-Manipulation
FPT_PHP.3	O.Phys-Probing O.Phys-Manipulation O.Leak-Forced O.Abuse-Func O.RND

11.2. Compatibility of the security functional requirements

According to the analysis presented in section 11.1, the compatibility of the security functional requirements is presented in the following table:

Table 15 Compatibility of the security functional requirements

Relevant Platform-ST SFRs	Composite-ST SFRs	Rationale
FAU_SAS.1	FAU_SAS.1	The platform provides the capability to load the Initialization Data and Pre-personalization Data to the TOE memory.
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES FCS_COP.1/ECC/DH FCS_COP.1/ECC/PACE_IM_ECDH	FCS_CKM.1/DH_PACE	The platform supports the security feature of TOE for ECDH key agreement and session key derivation during the PACE protocol.
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES FCS_COP.1/ECC/DH	FCS_CKM.1/CA	The platform supports the security feature of TOE for ECDH key agreement and session key derivation during Chip Authentication.
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_CKM.1/SCP	The platform supports the security feature of TOE for cryptographic key generation.
FCS_CKM.4/SCP FCS_CKM.4/SCL	FCS_CKM.4	The platform supports the security feature of TOE for cryptographic key destruction.
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES	FCS_COP.1/PACE_ENC	The platform supports the security feature of TOE to perform secure messaging – encryption and decryption in accordance with a specified Triple-DES or AES cryptographic algorithm.
FCS_COP.1/SCP/TDES FCS_COP.1/SCP/AES FCS_COP.1/SCL/TDES FCS_COP.1/SCL/AES	FCS_COP.1/CA_ENC	The platform supports the security feature of TOE to perform secure messaging – encryption and decryption in accordance with a specified Triple-DES or AES cryptographic algorithm.
FCS_COP.1/SCL/TDES-MAC FCS_COP.1/SCL/AES-MAC	FCS_COP.1/PACE_MAC	The platform supports the security feature of TOE to perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC or CMAC.

Relevant Platform-ST SFRs	Composite-ST SFRs	Rationale
FCS_COP.1/SCL/TDES-MAC FCS_COP.1/SCL/AES-MAC	FCS_COP.1/CA_MAC	The platform supports the security feature of TOE to perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC or CMAC.
FCS_COP.1/ECC/VER	FCS_COP.1/SIG_VER	The platform supports the security feature of TOE to perform digital signature verification with a specified cryptographic algorithm ECDSA.
FCS_COP.1/RSA/SIG_CRT	FCS_COP.1/AA_SIGN	The platform supports the security feature of TOE to perform digital signature creation for Active Authentication Data in accordance with a specified cryptographic algorithm RSA CRT.
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/SCP_ENC	The platform supports the security feature of TOE to perform secure messaging – encryption and decryption in accordance with a specified AES cryptographic algorithm.
FCS_COP.1/SCL/AES-MAC	FCS_COP.1/SCP_MAC	The platform supports the security feature of TOE to perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC.
FCS_COP.1/SCP/AES FCS_COP.1/SCL/AES	FCS_COP.1/SCP_KEY_DEC	The platform supports the security feature of TOE to perform on-card key sensitive data decryption in accordance with a specified AES cryptographic algorithm.
FCS_RNG.1/TRNG	FCS_RND.1	The platform provides the capability for TOE to generate random numbers.
FCS_RNG.1/TRNG	FIA_UAU.4/PACE	The platform supports the security feature of TOE to prevent reuse of authentication data.
FMT_LIM.1 FMT_LIM.2	FMT_LIM.1	The platform supports the security feature of TOE to provide protection against misuse of test features.

Relevant Platform-ST SFRs	Composite-ST SFRs	Rationale
FMT_LIM.1 FMT_LIM.2	FMT_LIM.2	The platform supports the security feature of TOE to provide protection against misuse of test features.
FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	FPT_EMS.1	The platform supports the TOE to detect the attacks based on inherent observable physical phenomena.
FRU_FLT.2 FPT_FLS.1	FPT_FLS.1	The platform supports the TOE to preserve a secure state when certain types of failures occur.
FPT_PHP.3	FPT_PHP.3	The platform supports the TOE to implement appropriate mechanisms to continuously counter physical manipulation and physical probing.
FRU_FLT.2 FPT_FLS.1 FPT_TST.2	FPT_TST.1	The platform supports the TOE to run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF and verify the integrity of the TSF data.

11.3. Compatibility of the security objectives for the TOE

According to the analysis presented in section 11.1, this section shows that the relevant security objectives of the Platform-ST are compatible with the ones of this Composite-ST with no contradictions. The mapping of the security objectives for the TOE is presented in the following table:

Table 16 Compatibility of the security objectives for the TOE

Relevant Platform-ST Objectives	Composite-ST Security objectives
O.Identification	OT.Identification
O.ECC	OT.Data_Integrity OT.Data_Authenticity OT.Data_Confidentiality OT.Sens_Data_Conf OT.Chip_Auth_Proof
O.TDES	OT.Data_Integrity OT.Data_Authenticity OT.Data_Confidentiality OT.Sens_Data_Conf OT.Chip_Auth_Proof

Relevant Platform-ST Objectives	Composite-ST Security objectives
O.AES-TDES-MAC	OT.Data_Integrity OT.Data_Authenticity OT.Data_Confidentiality OT.AC_Pers OT.Sens_Data_Conf OT.Chip_Auth_Proof
O.AES	OT.Chip_Auth_Proof OT.Data_Integrity OT.Data_Authenticity OT.Data_Confidentiality OT.Sens_Data_Conf OT.AC_Pers
O.RSA	OT.Active_Auth_Proof OT.Data_Authenticity
O.RND	OT.Data_Integrity OT.Data_Authenticity OT.Data_Confidentiality OT.AC_Pers OT.Sens_Data_Conf OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper
O.Abuse-Func	OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Abuse-Func OT.Prot_Malfunction OT.Data_Integrity OT.Prot_Phys-Tamper
O.Leak-Forced	OT.AC_Pers OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper OT.Data_Integrity
O.Leak-Inherent	OT.AC_Pers OT.Prot_Inf_Leak
O.Malfunction	OT.Prot_Inf_Leak OT.Prot_Malfunction
O.Phys-Manipulation	OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper OT.Data_Integrity
O.Phys-Probing	OT.Prot_Inf_Leak OT.Prot_Phys-Tamper OT.Data_Integrity

11.4. Compatibility of the security objectives for the operational environment

The following table determines the *significant* Security Objectives for the Operational Environment of Platform-ST and their relevance for the TOE.
The Security Objectives for the Operational Environment of Platform-ST are classified as three groups:

- **IrOE:** The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the base component.
- **CfPOE:** The objectives for the environment being fulfilled by the Composite-ST automatically.
- **SgOE**: The remaining objectives for the environment of the Platform-ST belonging neither to the group IrOE nor CfPOE. This group makes up the significant objectives for the environment for the composite-ST, which shall be addressed in the composite-ST.

Table 17 Tracing of Security Objectives of the Platform ST for Operational Environment

Security objectives of Platform ST for Operational Environment	**IrOE**	**CfPOE**	**SgOE**
OE.Resp-Appl		X	
OE.Process-Sec-IC	X		
OE.Lim_Block_Loader		X	
OE.Loader_Usage		X	
OE.TOE_Auth		X	
OE.Prevent_Masquerade		X	
OE.Secure_Load_ACode		X	

NOTE: The “OE.Process-Sec-IC” has been addressed by the assurance class ALC in the platform-ST.

Table 18 Mapping of Security Objectives of the Platform-ST for Operational Environment (CfPOE)

Security objectives of Platform ST for Operational Environment (CfPOE)	**Security objectives of Composite ST for TOE**	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
OE.Resp-Appl		X				X	X	X		X	X		X	
OE.Lim_Block_Loader										X				X
OE.Loader_Usage					X				X			X		
OE.TOE_Auth			X	X										
OE.Prevent_Masquerade						X	X	X		X				X
OE.Secure_Load_ACode					X									

11.5. Compatibility of the assurance requirements

The IC is certified at the assurance level EAL6+, which covers the security assurance requirements of the intended assurance level EAL5+ ALC_DVS.2 + AVA_VAN.5 of the composite TOE.

11.6. Results of compatibility analysis

The compatibility analysis is based on the evaluation of the relevance for the composite TOE of the parts of the Platform-ST. The relevance criteria have been determined according to ASE_COMP [30].
The rationale provided in the previous sections proved that there is no contradiction between the relevant parts of the Platform-ST and their counterparts in the Composite-ST.

12. References

12.1. Acronyms

AA	Active Authentication
AES	Advanced Encryption Standard
ASC	Application Secret Code
ASCII	American Standard Code for Information Interchange
BAC	Basic Access Control
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CBC	Cipher Block Chaining
CC	Common Criteria
CSCA	Country Signing Certification Authority
CV	Card Verifiable
CVCA	Country Verifying Certification Authority
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File

EIS	Extended Inspection System
ICAO	International Civil Aviation Organization
ICCSN	Integrated Circuit Card Serial Number.
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine readable zone
N/A	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PKI	Public Key Infrastructure
PP	Protection Profile
PT	Personalization Terminal
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SHA	Secure Hash Algorithm
SIP	Standard Inspection Procedure
SPA	Simple Power Analysis
ST	Security Target
TA	Terminal Authentication
TDES	Triple DES
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)

12.2. Glossary

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.
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [3], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [3] 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.
APDU	Application Protocol Data Unit, an ISO 7816-4 defined communication format between the card and the off-card applications. Cards receive requests for service from the CAD in the form of APDUs.
Application 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 [3] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System 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.
Biographic data (biodata).	The personalized details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document [3].
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 [3]
Country Signing CA Certificate (CSCA)	Certificate of the Country Signing Certification Authority Public Key (KPUCSCA) issued by Country Signing Certification Authority 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 having to be distributed by strictly secure diplomatic means, see [3]. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [3]) 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 [5].

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 [5]. 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 this ST. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [3]) 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 [5].
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 [5].
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 [3] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document 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 (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS).
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 (CDS), see [3] and [5]. This role is usually delegated to a Personalization Agent.
DPA	Differential Power Analysis is a form of side channel attack in which an attacker studies the power consumption of a cryptographic hardware device such as a smart card.

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.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [3]
Travel document (electronic)	The 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).
Extended Access Control	Security mechanism identified in [3] 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 the portrait.
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.
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 phases.
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 phase and embedded into the IC in the manufacturing life 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 Inlay&MRTD Manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
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.
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.4.4, TOE life-cycle, Phase 2, Step 3).
Initialisation 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 a State examining a travel document presented to it by a traveller (the travel document holder) and verifying its authenticity.
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller 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 Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer).
Issuing State	The Country issuing the travel document.
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [3]. 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 [2] as specified by ICAO on the contactless integrated circuit. It presents contactless 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 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.
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. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
NVRAM	Non-Volatile Random-Access Memory, a type of memory that retains its contents when power is turned off.
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.
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the Inlay&MRTD Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and Inlay&MRTD Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [4]. 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 [2] [3], • 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	(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 [3]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
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 "Enrolment" (cf. sec. 1.4.4, 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 [5], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [3] (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 including: (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 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.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Cryptographic authentication key used (i) by the Personalization Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.

Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): 1.biographical data, 2.data of the machine-readable zone, 3.photographic image and 4.other data.
Pre-Personalization	Process of writing Pre-Personalization Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.4.4, TOE life-cycle, Phase 2, Step 5)
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Inlay&MRTD Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
Pre-personalised travel document's chip	Travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the traveller is applying for entry.
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 [31].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [14]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [3], namely (i) PACE or BAC and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.

Terminal	A terminal is any technical system communicating with the TOE either through the contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising 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 [3] (there "Machine readable travel document").
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 [31] and programmed according to the Logical Data Structure as specified by ICAO [3] [2].
Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system 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 [19]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalization Agent from the Manufacturer.

User data	All data (being not authentication data): (i) stored in the context of the ePassport application of the travel document as defined in [5] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE . 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 [19]). 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 [20]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template.
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.

12.3. Technical References

[1] Network Working Group, RFC2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[2] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), Eighth Edition 2021.

[3] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs, Eighth Edition, 2021.

[4] INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents Part 12: Public Key Infrastructure for MRTDs, Eighth Edition, 2021.

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

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

[7] Security Target Lite - MK Lotus GovID IMDa V4.6.8.8 – Basic Access Control, V1.0, 2025-12-12.

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

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

[10] ICAO Applet Personalization Guide – Additional Information, V1.3.

[11] ePassport Applet Information, V1.8.

[12] Operational User Guidance, V1.8.

[13] Preparative Procedures, Version 1.9.

[14] ISO/IEC, International Standard 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, Edition 4, 2020-05.

[15] SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023.

[16] ISO/IEC, International Standard 9796-2, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, Edition 3, 2010-12.

[17] FIPS, NIST, FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012.

[18] BSI, Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012-06-28.

[19] CCMB, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 5, April 2017.

[20] CCMB, Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 5, April 2017.

[21] CCMB, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version 3.1, revision 5, April 2017.

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

[23] GlobalPlatform Inc., "GPC_SPE_014 GlobalPlatform Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D, Version 1.2," April 2020.

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

[25] Bundesamt für Sicherheit in der Informationstechnik, AIS 31: Funcrtionality Classes and Evaluation Methodology for Physical Random Number Generators, Version 1, 25.09.2001.

[26] Infineon, IFX_CCI_00002Dh,IFX_CCI_000039h,IFX_CCI_00003Ah, IFX_CCI_000044h,IFX_CCI_000045h,IFX_CCI_000046h,IFX_CCI_000047h,IFX_CCI_000048h,IFX_CCI_000049h,IFX_CCI_00004Ah,IFX_CCI_00004Bh,IFX_CCI_00004Ch,IFX_CCI_00004Dh,IFX_CCI_00004Eh T11 Security Target Lite, v6.5, 2024-08-20.

[27] Infineon, 32-bit Security Controller - V11, Security Guidelines, v1.00-2976, 2023-06-19.

[28] Infineon, 32-bit Security Controller - V11, Hardware Reference Manual, V6.2, 2020-12-21.

[29] BSI, BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, January 2014.

[30] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.

[31] ISO/IEC, International Standard 14443, Cards and security devices for personal identification – Contactless proximity objects, Edition 4, 2018.

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

[33] ISO/IEC, International Standard 7816-2, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts, Edition 2, 2007-10.

[34] GlobalPlatform Inc., "GlobalPlatform Card Specification, version 2.3.1," December 2017.

[35] "MKLotus-OS User Manual, V1.4".

[36] MK.QT.IT.13 Composite OS Production procedure, Version 01.

A. Platform identification

A.1. Identification of integrated circuits

The integrated circuits on which the TOE is based the secure microcontrollers IFX_CCI_000039h with firmware 80.306.16.0, including HSL v3.52.9708, UMSLC lib v01.30.0564, NRG SW 05.03.4097, SCL v2.15.000 and ACL v3.35.001.

The IC family received a Common Criteria certification at the EAL6 assurance level augmented with ALC_FLR.1 with certification ID:

- BSI-DSZ-CC-1107-V5-2024

The certificate of these integrated circuits is valid and up-to-date.

END OF DOCUMENT