KOMSCO

Security Target Lite

KCOS e-Passport Version 5.0

- SAC, EAC and AA on

S3D350A Family

KOMSCO

Date : 2019. 06. 10

Filename : EPS-05-AN-ST-SAC(Lite)

KOMSCO

Technology Research Institute

IT Research Department

The certified ST is written in Korean(including some English). This document is a translation of the original from Korean into English.

This page left blank on purpose for double-side printing.

KOMSCO Korea Minting, Security Printing & ID Card Operating Corp.	Revision History	Document	EPS-05-AN-ST-SAC(Lite)

개정번호	변경 내용	변경일	비고
1.0	New Publication	2019.06.10	

<Table of Contents>

<List of Tables>

<List of Figures>

1. ST Introduction (ASE_INT.1)

1.1. ST Reference

Title	Security Target <EPS-05-AN-ST-SAC(Lite)>
Date	2019.06.10
Version	1.0
Assurance Level	EAL5+ (ALC_DVS.2, AVA_VAN.5)
Protection Profile	BSI-CC-PP-0056-V2-2012, version 1.3.2, Dec 2012 [EACPassPP] BSI-CC-PP-0068-V2-2011-MA-01, version 1.01, Jul 2014' [PACEPassPP]
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Editor(s)	KOMSCO
Keywords	MRTD, e-Passport, SAC, EAC, AA, PACE, PACE-CAM

1.2. TOE Reference

TOE name	· KCOS e-Passport Version 5.0 - SAC, EAC and AA on S3D350A Family - K5.0.01.SS.D35A.02(S3D350A) - K5.0.01.SS.D30A.02(S3D300A) - K5.0.01.SS.D26A.02(S3D264A) - K5.0.01.SS.D23A.02(S3D232A)
TOE version	Version 5.0
TOE developer	KOMSCO
TOE Component	- IC chip : Samsung S3D350A Family[HWCR] (ANSSI-CC-2019/01) • including the IC Dedicated Crypto Library S/W - IC Embedded Software(OS) : KCOS e-Passport Version 5.0 – SAC, EAC and AA - The guidance documentation • EPS-05-QT-OPE-SAC-1.2 • EPS-05-QT-PRE-SAC-1.2

1 The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in Flash. These data are available by executing a dedicated command.

2 This identification data is described in the TOE guidance documentation. A more detailed explanation is described in the preparation guide(AGD-PRE)

1.3. TOE Overview

3 The TOE is the native chip operating system(COS), MRTD application and MRTD application data implemented on the IC chip and additionally includes S3D350A/300A/264A/232A version 2, which is a contactless IC chip of Samsung Electronics and is certified according to CC EAL 6+(ANSSI-CC-2019/01).

4 According to the Technical Guideline [EAC-TR] and [ICAO 9303], the ePassport Application supports Passive Authentication, Password Authenticated Connection Establishment (PACE), Terminal and Chip Authentication(EAC), Active Authentication(AA) and also Basic Access Control (BAC).

5 In this Security Target, BAC is not considered for evaluation.

6 the TOE also carries out the PAC (Personalization Access Control), which is a security mechanism for the secure personalization and management on the personalization phase at the Personalization Agent.

7 The main objectives of this ST are:

- To introduce TOE and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

8 The TOE uses generation of random numbers. TDES, AES, Retail MAC, CMAC, RSA and ECC supported by the MRTD chip. And the TOE can use RSA or ECC operations but the Personalization Agent has to select one cryptographic algorithm needed for EAC operation

9 Since The TOE is a composite evaluation product, it includes IC chip, COS, application programs, and etc. There is no non-TOE HW/FW/SW requested to perform TOE security attributes. Note, the RF antenna and the booklet are needed to represent a complete MRTD to ePassport holder, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.4. TOE Definition

10 The Target of Evaluation (TOE) addressed by the current security target is an electronic travel document representing a contactless smart card programmed according to Logical data structure (LDS) and protocols specified in [ICAO-9303] and additionally providing the Extended Access Control according to BSI TR-03110 part 1 and part 3 [EAC-TR] and Active Authentication according to [ICAO-9303]. 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 [PACEPassPP]. If Chip Authentication Mapping(PACE-CAM) as mapping of PACE protocol is performed, Terminal Authentication can be performed without Chip Authentication.

The TOE comprises of at least

- the circuitry of the travel document's chips(the integratedcircuit, IC)
- the IC Dedicated Software and the IC Dedicated Support Software
- the IC Embedded Software(operating system),
- the epassport application compliant with [ICAO-9303]
- the associated guidance documentation

1.4.1. TOE usage and security features for operational

11 A State or Organisation issues travel documents to be used by the holder for international travel. The traveller 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 traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

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

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

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

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

(c) the printed portrait.

(ii) **the logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [ICAO-9303] 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).

13 The issuing State or Organisation 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 organisational security measures (e.g. control of materials, personalisation procedures) [ICAO-9303]. These security measures can include the binding of the travel document's chip to the passport book.

14 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 Organisation and the security features of the travel document's chip.

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

16 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 [EAC-TR] as an alternative to the Active Authentication stated in [ICAO-9303].

17 BAC is also supported by the TOE, but this is not considered in the scope of this Security

Target due to the fact that BAC provides only resistance against enhanced basic attack potential (i.e. AVA_VAN.3).

18 The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature that shall be implemented by 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)' [PACEPassPP]. Note that this PP considers high attack potential.

19 For the PACE protocol according to [ICAO-9303], 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 K_{MAC} and K_{ENC} from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

20 After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [ICAO-9303], [EAC-TR].

21 The security target requires the TOE to implement Active Authentication described in [ICAO-9303]. This protocol provides evidence of the travel document' chip authenticity.

22 The security target requires the TOE to implement the Chip Authentication defineded in [EAC-TR]. The Chip Authentication prevents data traces described in [ICAO-9303]. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control or PACE, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (III) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by protocol properly. The Chip Authentication requires collaboration of the TOE and the TOE environment.

23 The security target requires the TOE to implement the Extended Access Control as defined in [EAC-TR]. 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.

24 **Application Note 1 :** In addition, the TOE supports PACE Chip Authentication Mapping (PACE-CAM) according to [ICAO-9303]. If PACE-CAM is performed, Terminal Authentication can be performed without explicit Chip Authentication beforehand. The secure messaging established by the PACE protocol is preserved to protect the data transmission from the TOE to the inspection system.

1.4.2. TOE Life Cycle

25 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP-IC-0084], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

26 Phase 1 “Development”

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

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

Phase 2 “Manufacturing”

(Step3) The TOE integrated circuit is produced by the IC manufacturereer conforming with KOMSCO requirements. The IC manufacturer writes the IC Identification Data onto the chip to control the IC during the IC as travel document material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacture to the MRTD manufacturer.

If necessary, the IC manufacturer adds the parts of the IC embedded Software in the non-volatile programmable memories (FLASH)

(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book.

(Step5) The MRTD manufacturer (i) Initializes the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.

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

Phase 3 “Personalisation of the travel document”

(Step6) The personalisation of the MRTD includes

(i) the survey of the MRTD holder’s biographical data,

(ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),

(iii) the printing of the visual readable data onto the physical part of the MRTD ,

(iv) the writing of the TOE User Data and TSF Data into the logical MRTD and

(v) configuration of the TSF if necessary.

The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of

(i) the digital MRZ data (EF.DG1),

(ii) the digitized portrait (EF.DG2), and

(iii) the Document security object.

The signing of the Document security object by the Document signer finalizes the personalisation of the genuine MRTD for the MRTD holder. The personalised MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 “Operational Use”

(Step7) The TOE is used as MRTD chip by the traveler and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note 2 : In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

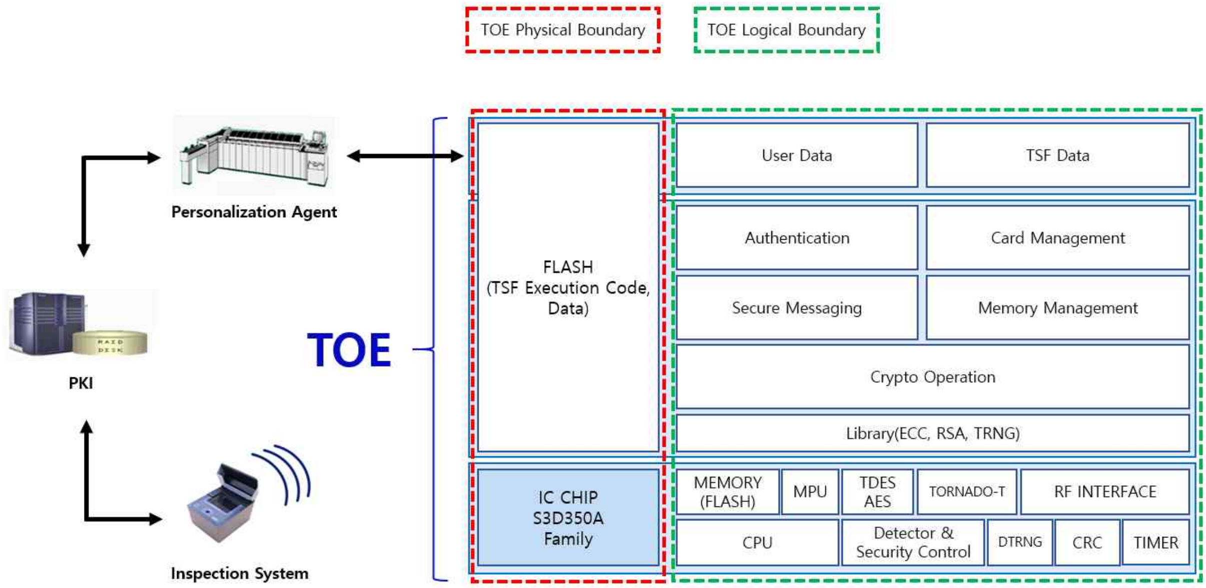
Actors

(Table 1-1) Identification of the actors

Actors	Identification
Integrated Circuit (IC) Developer	Samsung
Embedded Software Developer	KOMSCO
Integrated Circuit (IC) Manufacturer	Samsung
Code Image Downloader	KOMSCO or Samsung
Pre-personalizer	KOMSCO or Samsung
MRTD manufacturer	KOMSCO or another printer
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

The TOE is a composite evaluation product. For this reason, the evaluation of from (Step 1) to (Step 3) coverd by ALC assurance. And then, the process of delivery between ePassport/Inlay manufacturer, Personalization agent and ePassport holder is not included in the scope of this evaluation.

1.4.3. TOE Physical Boundaries



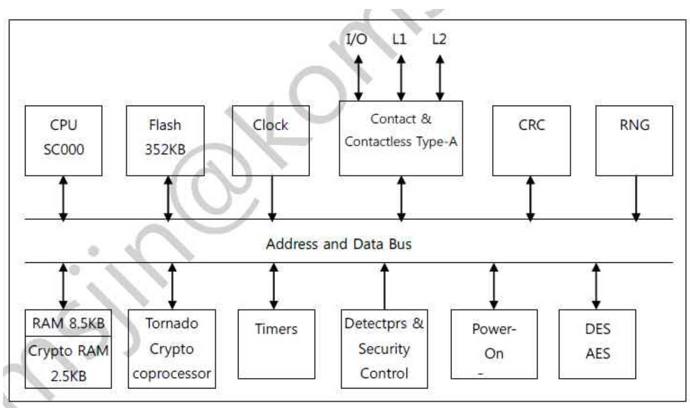
[Figure 1-1] TOE Physical/Logical Boundaries

The physical TOE is the following:

- the integrated circuit chip S3D350A Family(microcontoller) programmed with the operating system and with the ICAO application.

The components of chip are CPU, Crypto Co-Processor, I/O, Memory(RAM, FLASH), and various H/W functions.

In IC Chip's flash area, after e-passport application is installed, flash area is changed locked state.(Lock NVM attribute). And also, e-passport data like biomeric data (face, fingerprint) and TSF data(key for authentication, CA private key and AA private key) are saved in the flash area.



Samsung S3D350A Family which is the composition element of the IC chip, is a product certified with CCRA EAL 6+ assurance level, and the composition elements included in the authentication are IC chip hardware and cryptogaphic calculation software library as shown in the following.

<table>
<tr><th colspan="2">Classification</th><th>Identification information</th><th>Delivery form/method</th></tr>
<tr><td>TOE</td><td>IC Chip + COS + Application</td><td>· KCOS e-Passport Version 5.0 - SAC, EAC and AA on S3D350A Family
- K5.0.01.SS.D35A.02(S3D350A)
- K5.0.01.SS.D30A.02(S3D300A)
- K5.0.01.SS.D26A.02(S3D264A)
- K5.0.01.SS.D23A.02(S3D232A)</td><td>IC Chip (COB Format)/
by a person</td></tr>
<tr><td rowspan="4">TOE Components</td><td>IC Chip (HW)</td><td>S3D350A/S3D300A/S3D264A/S3D232A revision 2</td><td>wafer or module/
by a person</td></tr>
<tr><td>IC Dedicated SW</td><td>Secure Boot loader & System API Code v0.7
(07_S3D350A_Bootloader_SystemAPI_Release_v0_7_20170222.zip)
DTRNG FRO library v2.0
(S3D350A_DTRNG_FRO_Library_v2.0_LETI_delivery_20171012.zip)
AT1 Secure RSA/ECC/SHA Library v2.01
(20180802_PKA_lib_AT1_v2.01.zip)</td><td>Soft copy/
PGP email</td></tr>
<tr><td>COS+Application (SW)</td><td>KCOS e-Passport Version 5.0 – SAC, EAC and AA
· FLASH image
- KCOS50_350A.hex-1.3
- KCOS50_300A.hex-1.3
- KCOS50_264A.hex-1.3
- KCOS50_232A.hex-1.3
→ included certified crypto library of IC chip</td><td>FLASH code/
PGP email</td></tr>
<tr><td>DOC</td><td>- AGD_OPE : EPS-05-QT-OPE-SAC-1.2
- AGD_PRE : EPS-05-QT-PRE-SAC-1.2</td><td>Soft copy or Book/
PGP email or a person</td></tr>
</table>

1.4.4. TOE Logical Boundaries

KCOS e-Passport Version 5.0 − SAC, EAC and AA operating system manages all the resources of the integrated circuit that equips the passport, providing secure access to data and functions. Major tasks performed by operating system are:

- Communication with external deivces(Inspection System and Personalization Agent)
- Data storage in the file system and secure memory area
- Dispatch and execution of commands
- Cryptographic operation
- Management of the security policies

Logical area in Figure 1-1 shows an overview of the TOE architecture.

- Crypto Operation : provides the cryptographic services(3-DES, AES, SHA, MAC, RSA, ECC etc.)
- Authentication : loading of keys related to authentication and the function of authentication such as PAC, SAC, AA, EAC
- Card Management : sending and receiving of APDU, integrity checking, clearing of residual information and the function for preservation of TOE secure state
- Memory Management : creating, selection, deleting of files and management of transaction
- Secure Messaging : securemessaging for secure communication channel
- User Data : All data(being not authentication data) stored in the context of the ePassport application of travel document as defined in [EAC-TR] and [ICAO-9303] such as EF.DG1, EF.DG2, EF.DG5 ~ EF.DG16)
- TSF Data : Data created by and for the TOE that might affect the operation of the TOE including the private authentication key such as Private Chip Authentication Key and Private Active Authentication Key

Security Mechanism

27 The TOE provides security features such as confidentiality, integrity, access control and authentication for e-Passport personalization data and TSF data security. These security features implemented as SAC and EAC security mechanism which defined [ICAO-9303] and [EAC-TR] and PAC security mechanism for personalization. Also, The TOE consists of PA authentication

for detect e-Passport personalization data forgery through digital signature verification of SOD which is from TOE to verification system and AA authentication features.

< PAC(Personalization Access Control) >

28 The TOE provides the PAC security mechanism which consists of PAC mutual authentication and PAC session key generation used for access control of Personalization Agent in initialization phase and personalization phase.

29 The PAC authentication is entity authentication protocol based on TDES/AES to authenticate between Personalization Agent and TOE in personalization phase. The PAC authentication uses TDES/AES algorithm. However, according to Application note 31 at [BACPassPP], it does not include 2-KEY based TDES algorithm for evaluation scope.

30 The PAC session key generation feature is to make PAC session key(i.e. PAC session crypto key and PAC session MAC key) in order to create secure channel between TOE and Personalization Agent. The PAC session key generation is implemented by key derivation protocol based on TDES/AES. The way to create secure channel is similar to that of the BAC mechanism.

< SAC(Supplemental Access Control) >

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

32 PACE establishes secure messaging between an travel-document chip and an inspection system based on possibly weak (short) passwords. The security context is established in the EF.CardAccess. The protocol enables the travel-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).

33 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.

34 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.

35 All the algorithm combinations (i.e. key agreement algorithms, mapping algorithms, block ciphers) and the standardized domain parameters specified in [ICAO-9303] are supported for PACE authentication.

< PA(Passive Authentication)>

36 The integrity of data stored under the LDS is checked by means of the Passive Authentication mechanism defined in [ICAO-9303]. Passive Authentication consists of the following steps :

1. The inspection system reads the Document Security Object (SOD), which contains the Document Signer Certificate 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).
3. The inspection system uses the verified Document Signer Public Key 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).

< AA(Active Authentication) >

37 Active Authentication authenticates the IC by signing a challenge sent by the inspection system with a private key known only to the IC[ICAO-9303].
For this purpose, the IC contains its own Active Authentication key pair. A hash representation of Data Group 15 (public key info) is stored in the Document Security Object (SOD), and is therefore authenticated by the issuer's digital signature. The corresponding private key is stored in the IC secure memory.

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

< EAC(Extended Access Control) >

▢ **EAC-CA**

38 Chip Authentication is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the the travel-document chip [ICAO-9303]. The main differences with respect to Active Authentication is :

- Besides authentication of the e-Document chip, this protocol also provides strong session keys.

Details on Challenge Semantics are described in [ICAO-9303].

The static Chip Authentication key pair(s) must be stored on the travel-document chip.

- 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 travel-document chip itself and the stored data by performing secure messaging with the new session keys.

▢ **EAC-TA**

39 Extended Access Control is a security mechanism by means of which the travel-document chip authenticates the inspection systems authorized to read the optional biometric reference data and protects access to these data.
Following [EAC-TR], 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 travel 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 or PACE with Chip Authentication Mapping. In this way, the travel 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 travel 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 travel 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.

Additional Security Features

40 The TOE provides crypto operation, identification, authentication and access control through the PAC and SAC secure mechanism.
The TOE manages the function such as Initialization, Pre-personalisation, Personalisation and managing TSF data such as crypto key for security mechanism and certifications. Also, The TOE manages the security role such as Manufacturer, Personalisation Agent, Terminal.
The TOE performs self test and provides integrity check way to ensure secure operation. While in operation, The TOE operates countermeasure from DPA/SPA technique which is extracting crypto information by analysing the physical phenomenon(such as current, voltage, electro-magnetic). Also, it provides protection countermeasure from physical invasion.

IC Chip Providing Features

IC chip is composed of a processing unit, security components, contactless and contact based I/O ports. IC chip also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including optional public key cryptographic libraries, a random number generation library and an random number generator. The public key cryptographic libraries further include the functionality of hash computation.

IC chip also supports the feature :

security Security sensors, detectors or filters

- Shields
- Life time detector
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks

(Table 1-2) The main feature of IC chip and usage in TOE

The feature of IC chip		usage in TOE
Security	• TDES	○
	• AES	○
	• RSA • ECC	○
	• SHA-2	○
	• RNG	○(DTRNG)
	• Abnormal condition detectors	○
	• MPU	○
	• MEMORY ENCRYPTION	○
	• Random Branch Insertion(RBI)	○
	• Variable Clock	○
Communication	• ISO7816 contact interface	X
	• ISO14443 contactless interface	○

2. Conformance Claims (ASE_CCL.1)

2.1. CC Conformance Claim

41 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

- Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,
- Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,
- Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

as follows:

- Part 2 extended,
- Part 3 conformant.

42 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017 ([CC]) has to be taken into account. The evaluation follows the Common Evaluation Methodology (CEM) with current final interpretations.

2.2. PP Claim

43 This ST claims strict conformance to 'Common Criteria Protection Profile Machine Read-able Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056-V2-2012, version 1.3.2', December 2012 [EACPassPP].

44 This ST claims strict conformance to 'Common Criteria Protection Profile Machine Read-able Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01, version 1.01, July 2014' [PACEPassPP].

Application Note 3 : The IC chip, which is a component of the TOE, complies with the Security IC Platform Protection Profile with Augmentation Packages, Version 1.0 (BSI-CC-PP-0084-2014). Refer to ST[HWST] of the IC chip for rationale of conformance to this PP.

2.3. Package Claim

45 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [HWCR]. The IC hardware platform and its primary embedded software are evaluated at level EAL 6+.

46 The evaluation assurance level of the TOE is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 as defined in [CC].

2.4. Conformance Statement

47 This ST strictly conforms to [PACEPassPP] and [EACPassPP].

3. Security Problem Definition (ASE_SPD.1)

3.1. Introduction

3.1.1. Assets

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

1) Assets listed in PP PACE

49 The primary assets to be protected by the TOE as long as they are in scope of the TOE are listed in Table 3-1 (please refer to the glossary in chap 8 for the term definitions).

(Table 3-1) Primary assets

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 [ICAO-9303] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-9303]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BACPassPP]	Confidentiality[1)] 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 [ICAO-9303] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-9303]). 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 recognising the TOE not knowing any PACE password. TOE tracing data can be provided/gathered.	unavailability[2)]

Application Note 4 : 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.

50 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:

(Table 3-2) Secondary assets

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 authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised 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 [BACPassPP].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to	Confidentiality Integrity

1) Though not each data element stored on the TOE represents a secret, the ICAO Specification [ICAO-9303] anyway requires securing their confidentiality: only terminals authenticated according to [ICAO-9303] can get access to the user data stored. They have to be operated according to P.Terminal.
2) represents a prerequisite for anonymity of the travel document holder

		enforce its security functionality.	
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 authorisation data	Restricted-revealable[3)] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

Application Note 5 : Since the travel document does not support any secret document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE authentication of a terminal does not unambiguously mean that the travel document holder is using TOE.

Application Note 6 : travel document communication establishment authorisation 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 authorisation attempt.

51 The TOE shall secure the reference information as well as −. together with the terminal connected - the verification information in the “TOE ⇔ terminal” channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be sent to the TOE. The secondary assets represent TSF and TSF-data in the sense of CC.

2) Assets listed in PP EAC

52 The assets to be protected by the TOE include the User Data on the travel document’s chip, user data transferred between the TOE and the terminal, and travel document tracing data from the claimed PACE PP [PACEPassPP], chap 3.1.

3) The travel document holder may reveal, if necessary, verification values of the CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.

Logical travel-document sensitive User Data

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

54 Due to interoperability reasons the ICAO Doc 9303 [ICAO 9303] 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 according to this ST, if it is accessed using BAC [ICAO 9303] (conformance to the BAC certification [R1] is kept, though). Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [BACPasspp]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as these mechanisms are resistant to high attack potential.

55 A sensitive asset is the following more general one.

Authenticity of the travel-document's chip

56 The authenticity of the travel-document's chip personalised by the issuing State or Organization for the travel-document holder is used by the presenter to prove his possession of a genuine travel-document.

3.1.2. Subjects

57 This security target considers the subjects defined in the PACE PP[PACEPassPP], and in the EAC PP[EACPassPP]. The subjects considered in accordance with the PACE PP[PACEPassPP] are listed in Table 3-3.

(Table 3-3) Subjects and external entities according to PACE PP

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [BACPassPP]. Please note that a travel document holder can attacker.
2	-	travel document presenter(traveller)	A person presenting the travel document to a terminal and claiming the identity of the travel document holder[4].

			This external entity is commensurate with 'Traveller' in [BACPassPP]. Please note that a travel document presenter can also be an attacker.
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [BACPassPP].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[5)] 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 organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [ICAO-9303]. This role is usually delegated to a Personalisation Agent.
6	-	Country Signing Certification Authority (CSCA)	An organisation 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(C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [ICAO-9303].
7	4	Personalization Agent	An organisation acting on behalf of the travel document Issuer to personalise 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 personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO-9303]. (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BACPassPP].
8	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [BACPassPP].
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 recognised by the TOE. This external entity is commensurate with 'Attacker' in [BACPassPP].

4) i.e. this person is uniquely associated with a concrete electronic travel document
5) Concretely, by a control officer

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

Country Verifying Certification Authority

59 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

60 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 Organisations in the form of the Document Verifier Certificates.

Terminal

61 A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface.

Inspection system (IS)

62 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.

Extended Inspection System (EIS)

63 The **Extended Inspection System (EIS)** performs the Advanced Inspection Procedure (Figure 3-1) 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 [EAC-TR] and

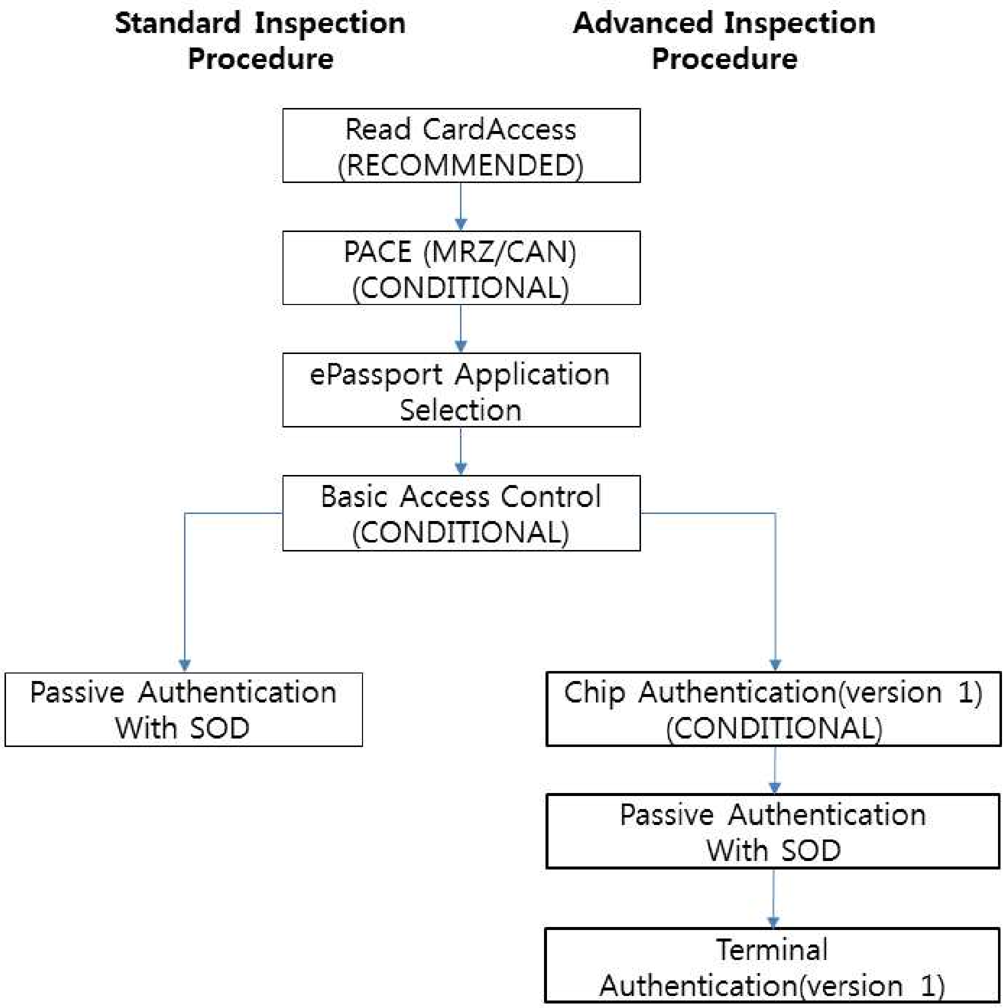
(v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

64 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

65 Additionally to the definition in Table 3-3, the definition of an attacker is refined as follows: A threat agent trying (i) to manipulate the logical travel document without authorisation, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel documentor (iv) to trace an travel document.

Application Note 7 : 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.



[Figure 3-1] Authentication procedures for the ePassport Application

66 The Chip Authentication step in Figure 3-1 is skipped if a PACE-CAM authentication has been successfully performed.

3.1.3. Assumptions

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

- **A.Passive_Auth PKI for Passive Authentication**

68 The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel

document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity.

The Document Signer

(i) generates the Document Signer Key Pair,

(ii) hands over the Document Signer Public Key to the CA for certification,

(iii) keeps the Document Signer Private Key secret and

(iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303].

- **A.Insp_Sys Inspection Systems for global interoperability**

69 The Extended Inspection System (EIS) for global interoperability

(i) includes the Country Signing CA Public Key and

(ii) implements the terminal part of PACE [ICAO-9303] and/or BAC [BACPassPP].

BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. The Chip Authentication Protocol v.1 is skipped if PACE-CAM has previously been performed. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

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

- **A.Auth_PKI PKI for Inspection Systems**

70 The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification

Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

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 [PACEPassPP] 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.

3.2. Threats

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

- **T.Skimming Skimming travel-document/Capturing Card-Terminal Communication**

72 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 contact or contactless interfaces 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 8 : A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

Application Note 9 : 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.

• **T.Eavesdropping Eavesdropping on the communication between the TOE and the PACE terminal**

73 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 10 : A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

• **T.Tracing Tracing travel document**

74 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/contact interface of the TOE.

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

Asset : privacy of the travel document holder

Application Note 11 : This Threat completely covers and extends “T.Chip-ID” from BAC PP [BACPassPP].

Application Note 12 : 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.

Application Note 13 : Since the Standard Inspection Procedure does not support any unique secret-based authentication of the travel document’s chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.

• **T.Forgery Forgery of Data**

75 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

- **T.Abuse-Func Abuse of Functionality**

76 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 initialisation and personalisation in the operational phase after delivery to the travel document holder.

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

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

Application Note 14 : 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.

- **T.Information_Leakage Information Leakage from travel document**

77 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 15 : 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).

- **T.Phys-Tamper Physical Tampering**

78 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 16 : 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.

• **T.Malfunction Malfunction due to Environmental Stress**

79 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 17 : 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.

• **T.Read_Sensitive_Data Read the sensitive biometric reference data**

80 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 (cf. [BACPassPP]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

Threat agent : having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document

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

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

81 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 traveller by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

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

Asset : authenticity of user data stored on the TOE

Application note 18 : T.Forgery from the PACE PP [PACEPassPP] shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

3.3. Organizational Security Policies

82 The TOE and/or its environment shall comply to the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

- **P.Manufact Manufacturing of the travel document's chip**

83 The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

- **P.Pre-Operational Pre-operational handling of the travel document**

84 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 authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

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

85 **Application Note 19 :** The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}) .
2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [ICAO-9303]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [ICAO-9303].
3) A Document Signer shall
   (i) generate the Document Signer Key Pair,
   (ii) hand over the Document Signer Public Key to the CSCA for certification,
   (iii) keep the Document Signer Private Key secret and
   (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

- **P.Trustworthy_PKI Trustworthiness of PKI**

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

- **P.Terminal Abilities and trustworthiness of terminals**

87 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 [ICAO-9303].
2) They shall implement the terminal parts of the PACE protocol [ICAO-9303], of the Passive Authentication [ICAO-9303] and use them in this order[6)] The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3) The related terminals need not to use any own credentials.
4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO-9303].
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.

- **P.Sensitive_Data Privacy of sensitive biometric reference data**

88 The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

6) This order is commensurate with [ICAO-9303].

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

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

- **P.Activ_Auth Active Authentication**

90 The TOE implements the active authentication protocol as described in [ICAO-9303].

4. Security Objectives (ASE_OBJ.2)

91 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.

4.1. Security Objectives for the TOE

92 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.

- **OT.Data_Integrity Integrity of Data**

93 The TOE must ensure integrity of the User Data and the TSF-data[7] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).

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

- **OT.Data_Authenticity Authenticity of Data**

94 The TOE must ensure authenticity of the User Data and the TSF-data[8] stored on it by enabling verification of their authenticity at the terminal-side[9].

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)[10].

- **OT.Data_Confidentiality Confidentiality of Data**

95 The TOE must ensure confidentiality of the User Data and the TSF-data[11] by granting read

7) where appropriate, see Table 3-2 above
8) where appropriate, see Table 3-2 above
9) Verification of SOD
10) Secure messaging after PACE authentication, see also [ICAO-9303]
11) where appropriate, see Table 3-2 above

access only to the PACE authenticated BIS-PACE connected.

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

- **OT.Tracing Tracing travel document**

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

- **OT.Prot_Abuse-Func Protection against Abuse of Functionality**

97 The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order

(i) to manipulate or to disclose the User Data stored in the TOE,

(ii) to manipulate or to disclose the TSF-data stored in the TOE,

(iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

- **OT.Prot_Inf_Leak Protection against Information Leakage**

98 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 20 : This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

- **OT.Prot_Phys-Tamper Protection against Physical Tampering**

99 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.

- **OT.Prot_Malfunction Protection against Malfunctions**

100 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.

101 The following TOE security objectives (OT.Identification, OT.AC_Pers) address the aspects of identified threats to be countered involving TOE's environment.

- **OT.Identification Identification of the TOE**

102 The TOE must provide means to store Initialisation[12] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

- **OT.AC_Pers Access Control for Personalisation of logical MRTD**

103 The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO-9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

12) Amongst other, IC identification data

Application Note 21 : The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

- **OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data**

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

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

105 The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of either the PACE-CAM as defined in [ICAO-9303] or the Chip Authentication Version 1 as defined in [EAC-TR]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application Note 22 : 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 [ICAO-9303] and

(ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

- **OT.Active_Auth_Proof Proof of travel document's chip authenticity by AA**

106 The TOE must support the Basic Inspection Systems to verify the identity and authenticity of

the travel-document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303]. The authenticity proof through AA provided by travel-document's chip shall be protected against attacks with high attack potential.

4.2. Security Objectives for the Operational Environment

Travel document Issuer as the general responsible

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

- **OE.Legislative_Compliance Issuing of the travel document**

108 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

109 The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 19 above):

- **OE.Passive_Auth_Sign Authentication of travel document by Signature**

110 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 (C_{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 [ICAO-9303]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO-9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

- **OE.Personalisation Personalisation of travel document**

111 The travel document Issuer must ensure that the Personalisation Agents acting on his behalf

(i) establish the correct identity of the travel document holder and create the biographical data for the travel document,

(ii) enrol the biometric reference data of the travel document holder,

(iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO-9303] ,

(iv) write the document details data,

(v) write the initial TSF data,

(vi) sign the Document Security Object defined in [ICAO-9303] (in the role of a DS).

Terminal operator: Terminal's receiving branch

- **OE.Terminal Terminal operating**

112 The terminal operators must operate their terminals as follows:

1) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [ICAO-9303].

2) The related terminals implement the terminal parts of the PACE protocol [ICAO-9303], of the Passive Authentication [ICAO-9303] (by verification of the signature of the Document Security Object) and use them in this order37. 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 C_{CSCA} and C_{DS}) 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, [ICAO-9303]).

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.

Application Note 23 : OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from BAC PP [BACPassPP].

Travel document holder Obligations

- **OE.Travel_Document_Holder Travel document holder Obligations**

113 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 Organisation

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

- **OE.Auth_Key_Travel_Document Travel document Authentication Key**

115 The issuing State or Organisation has to establish the necessary public key infrastructure in order to

(i) generate the travel document’s Chip Authentication Key Pair,

(ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and

(iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document’s chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Justification : This security objective for the operational environment is needed additionally to those from [PACEPassPP] 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 this Security Target. and not in [PACEPassPP].

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

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

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

117 The following Security Objective for the Operational Environment is an addition to the objectives given by the Protection Profiles to cover the Active Authentication mechanism.

• **OE.Active_Auth_Key_travel-document travel-document Active Authentication key**

118 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.

Justification : This security objective for the operational environment is needed additionally to those from [PACEPassPP]/[EACPassPP] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Active Authentication which is one of the additional features of the TOE described only in this ST and not in [PACEPassPP]/[EACPassPP].

Receiving State or Organisation

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

- **OE.Exam_Travel_Document Examination of the physical part of the travel document**

120 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 and/or the Basic Access Control. Extended Inspection Systems perform additionally to these points the Chip Authentication as either part of PACE-CAM or as 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 in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication as either part of PACE-CAM or as Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal and therefore also counters T.Forgery and A.Passive_Auth. This is done because this ST introduces the Extended Inspection System which is needed to handle the additional features of a travel document with Extended Access Control.

- **OE.Prot_Logical_Travel_Document Protection of data from the logical travel document**

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

Justification : This security objective for the operational environment is needed in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication.

• **OE.Ext_Insp_Systems Authorization of Extended Inspection Systems**

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

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

4.3. Security Objective Rationale

123 The following table 4-1 provides an overview for security objectives coverage (TOE and its environment). 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.

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

125 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 or contact interface. This threat is countered by the security objectives **OT.Data_Integrity**, **OT.Data_Authenticity** and **OT.Data_Confidentiality** through the PACE authentication. The objective **OE.Travel_Document_Holder** ensures that a PACE session can only be established either by the travel document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

126 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.

(Table 4-1) security objectives rationale

	OT.Sens Data Conf	OT.Chip Aut 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 Malfunction	OE.Auth Key Travel Document	OE.Active Auth Key Travel 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			
P.Active_Auth			X												X									
A.Insp_Sys	N/A																X	X						
A.Auth_PKI																X			X					
A.Passive_Auth																	X				X			

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

128 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 Personalisation Agent (cf. **OE.Personalisation**). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives **OT.Data_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. 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.

129 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.

130 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.

131 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 Organisation. 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 as either part of PACE-CAM or as Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip.

In addition, the threat **T.Counterfeit** "Counterfeit of the travel document chip data" is countered by chip an identification and authenticity proof required by **OT.Active_Auth_Proof**

"Proof of travel document's chip authenticity by AA" using an 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_Travel_Document** "the travel document Authentication Key".

132 The OSP **P.Manufact** "Manufacturing of the travel document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalisation Data as being fulfilled by **OT.Identification**.

133 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.Personalisation** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorisation of Personalisation Agents' : **OE.Legislative_Compliance** is affine to the OSP's property 'compliance with laws and regulations'.

134 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).

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

136 The OSP **P.Personalisation** "Personalisation of the travel document by issuing State or Organisation only" addresses the

(i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** "Personalisation of logical travel document", and

(ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document".

Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation Agent.

137 The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the

TOE-objective **OT.Sens_Data_Conf** “Confidentiality of sensitive biometric reference data” requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by **OE.Authoriz_Sens_Data** “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** “Authorization of Extended Inspection Systems”.

138 The OSP **P.Terminal** “Abilities and trustworthiness of terminals” is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [PACEPassPP] **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol. and also, The OSP **P.Terminal** is obviously enforced by the objective **OE.Terminal,** whereby the one-to-one mapping between the related properties is applicable.

139 In addition, the OSP **P.Active_Auth** is countered by chip an identification and authenticity proof required by **OT.Active_Auth_Proof** “Proof of travel document’s chip authenticity by AA” using an 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_Travel_Document** “the travel document Authentication Key”.

140 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, or the Basic Inspection System with PACE to implement the PACE, 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.

141 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 [PACEPassPP] 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”.

142 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.

5. Extended Components Definition (ASE_ECD.1)

143 This ST uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0084]; others are defined in the protection profile [EACPassPP] and [PACEPassPP].

5.1. Definition of the family FAU_SAS

144 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:

(Table 5-1) Family FAU_SAS

FAU_SAS Audit data storage	
Family behaviour:	This family defines functional requirements for the storage of audit data.
Component leveling:	
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data
Management	There are no management activities foreseen.
Audit	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: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

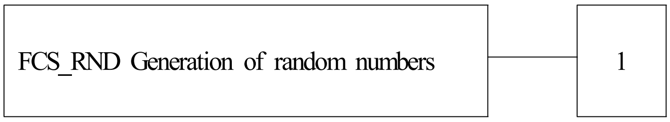
5.2. Definition of the family FCS_RND

145 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

noncryptographic use.

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

(Table 5-2) Family FCS_RND

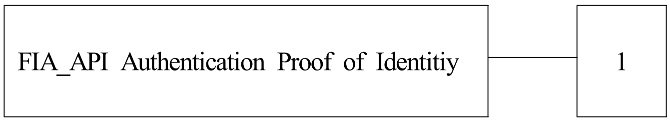
FCS_RND Generation of random numbers	
Family behaviour:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component leveling:	
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management	There are no management activities foreseen.
Audit	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*].

5.3. Definition of the family FIA_API

146 To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [PACEPassPP]. 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 (cf. [CC], chapter “Explicitly stated IT security requirements (APE_SRE)”) from a TOE point of view.

(Table 5-3) Family FIA_API

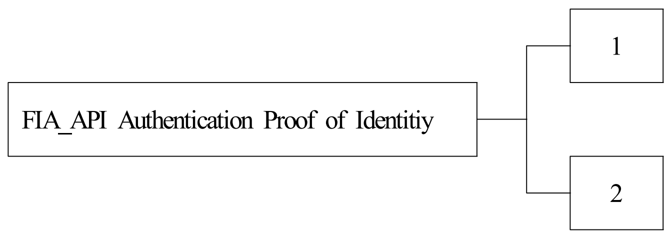
FIA_API Authentication Proof of Identity	
Family behaviour:	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
Component leveling:	
FIA_API.1	**Authentication Proof of Identity.**
Management	The following actions 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 rule*].

5.4. Definition of the family FMT_LIM

147 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

(Table 5-4) Family FMT_LIM

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 the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
Component leveling:	
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.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable
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	There are no management activities foreseen.
Audit	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

5.5. Definition of the family FPT_EMS

148 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 [CC].

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

(Table 5-5) Family FPT_EMS

FPT_EMS TOE Emanation	
Family behaviour:	This family defines requirements to mitigate intelligible emanations.

Component leveling:	
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	There are no management activities foreseen.
Audit	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 TSF 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].

6. Security Requirements (ASE_REQ.2)

149 This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

150 The CC allows several operations to be performed on functional requirements; refinement, *selection, assignment,* and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC]. Each of these operations is used in this ST.

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

152 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined text. and the original text of the compnent is given by a footnot. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and underlined text with “<” like <this>.

153 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 and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized with “<” like <*this*>.

154 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.

155 The definition of the subjects “Manufacturer”, “Personalisation Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used

in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 8 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC]. The operation “load” is synonymous to “import” used in [CC].

(Table 6-1) Definition of security attributes

Security attribute	Values	Meaning
Terminal authentication status	None (any Terminal)	Default role (i.e. without authorisation after start-up)
	CVCA	Roles defined in the certificate used for authentication (cf. [EAC-TR]); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA.
	DV (domestic)	Roles defined in the certificate used for authentication (cf. [EAC-TR]); Terminal is authenticated as domestic Document Verifier after successful CA and TA.
	DV (foreign)	Roles defined in the certificate used for authentication (cf. [EAC-TR]); Terminal is authenticated as foreign Document Verifier after successful CA and TA.
	IS	Roles defined in the certificate used for authentication (cf. [EAC-TR]); Terminal is authenticated as Extended Inspection System after successful CA and TA.
Terminal Auth orization	none	
	DG4 (Iris)	Read access to DG4 (cf. [EAC-TR]).
	DG3 (Fingerprint)	Read access to DG3 (cf. [EAC-TR]).
	DG3(Fingerprint)/DG4(Iris)	Read access to DG3 and DG4 (cf. [EAC-TR]).

156 The following table provides an overview of the keys and certificates used.

(Table 6-2) Keys and certificates

Name	**Data**
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Receiving PKI branch	
Country Verifying Certification Authority	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.

Private Key (SK_{CVCA})	
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [EAC-TR, Glossary]). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) ssued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}) (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Issuing PKI branch	
Country Signing Certification Authority KeyPair and Certificate	Country Signing Certification Authority of the travel document Issuer signs the Document Signer Public Key Certificate (C_{DS}) with the Country Signing Certification Authority Private Key (SK_{CSCA}) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK_{CSCA}). The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) to be distributed by strictly secure diplomatic means, see. [ICAO-9303].
Document Signer Key Pairs and Certificates	The Document Signer Certificate C_{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK_{DS}) as authentication reference data. The Document Signer acting

	under the policy of the CSCA signs the Document Security Object (SO_D) of the travel document with the Document Signer Private Key (SK_{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK_{DS}).
Chip Autentication Public Key Pair	The Chip Authentication Public Key Pair(SK_{ICC}, PK_{ICC}) are used for Key Agrrement Protocol; Diffie-Hellman(DH) according to RFC2631 or Elloptic Curve Diffie-Hellman according to [ISO 11770-3]
Chip Authentication Public Key (PK_{ICC})	PK_{ICC} is stored in EF.DG14 on the TOE's logical travel document and used by the terminal for Chip Authentication. Its authenticity is verified by terminal in the context of the Passive Authentication (verification of SO_D). It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Key Pair(SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip.
Active Authentication Key Pair	The Active Authentication Key Pair(PK_{AA},SK_{AA}) is used for the Active Authentication mechanism in accordance with [ICAO-9303].
Active Authentication Public Key (PK_{AA})	The Active Authentication Public Key (PK_{AA}) is stored in the EF.DG15. These keys are used by Inspection Systems to confirm the genuinity of the travel document's chip.
Active Authentication Private Key (SK_{AA})	The Active Authentication Private Key (SK_{AA}) is used by the TOE to authenticate itself as genuine the travel document's chip.
PACE Chip Authentication Mapping Public Key Pair	The PACE Chip Authentication Mapping Public Key Pair (SK_{CAM}, PK_{CAM}) are used for PACE Chip Authentication Mapping according to [ICAO-9303], [EAC-TR].
PACE Chip Authentication Mapping Public Key (PK_{CAM})	The PACE Chip Authentication Mapping Public Key (PK_{CAM}) is stored in the EF.CardSecurity of the TOE''s logical travel document and used by the inspection system for PACE Chip Authentication Mapping of the travel document''s chip. It is part of the User Data provided by the TOE for the IT environment.
PACE Chip Authentication Mapping Private Key (SK_{CAM})	The PACE Chip Authentication Mapping Private Key (SK_{CAM}) is used by the TOE to authenticate itself as authentic travel document''s chip.
Session keys	
PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or 3-DES Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [ICAO-9303]
PAC Session Keys	Secure messaging AES keys for message authentication (CMAC-mode)

($PAC\text{-}K_{MAC}$, $PAC\text{-}K_{ENC}$)	and for message encryption (CBC-mode) or 3-DES Keys for message authentication(Retail MAC) and message encryption (CBC) agreed between the TOE and a personalization agent as result of the PAC Protocol in order to write the TOE User Data and TSF Data into the TOE.
Chip Authentication Session Keys ($CA\text{-}K_{MAC}$, $CA\text{-}K_{ENC}$)	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
Ephemeral keys	
PACE authentication ephemeral key pair ($ephem\text{-}SK_{PICC}\text{-}PACE$, $ephem\text{-}PK_{PICC}\text{-}PACE$)	The ephemeral PACE Authentication Key Pair ($ephem\text{-}SK_{PICC}\text{-}PACE$, $ephem\text{-}PK_{PICC}\text{-}PACE$) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to [EAC-TR].

Application Note 26 : The Country Verifying Certification Authority identifies a Document Verifier as “domestic” in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as “foreign” in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD’s point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.1. Security Functional Requirements for the TOE

157 This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1. Class FAU Security Audit

158 The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (CC part 2 extended).

FAU_SAS.1 Audit storage

159 Hierarchical to: No other components.

Dependencies: No dependencies

FAU_SAS.1.1	The TSF shall provide the Manufacturer[13] with the capability to store the the Initialization and Pre-Personalization Data[14] in the audit records.

Application Note 27 : The Manufacturer role is the default user identity assumed by the TOE in the life phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.2. Class FCS Cryptographic Support

160 The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (CC part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

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

161 Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or

FCS_COP.1 Cryptographic operation]:

Justification : A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_CKM.1.1/DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: 1. <Diffie-Hellman Protocol compliant to PKCS#3 **[RSA-PKCS#3]**>[15] and specified cryptographic key sizes: <*2048 bits*>[16], and 2. <ECDH compliant to **[EAC-TR]**>[17] and specified cryptographic key sizes: <*192, 224, 256, 320, 384, 512 bits*>[18], that meet the following: **[ICAO-9303]**[19]

13) *[assignment: authorized users]*
14) *[assignment: list of audit information]*

Application Note 28 : The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO-9303]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS#3]) or on the ECDH compliant to TR-03111 [ECC-TR] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [ICAO-9303] and [EAC-TR] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}) according to [ICAO-9303] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application Note 29 : FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO-9303].

Application Note 30 : The TOE supports the following standardized elliptic curve domain parameters (cf. [EAC-TR, part 3 Table 4]):

(Table 6-3) Supported Standard Domain Parameters

ID	Name	Size
1	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224
2	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256
3-7	RFU	
8	NIST P-192(secp192r1)	192
9	BrainpoolP192r1	192
10	NIST P-224(secp224r1)	224
11	BrainpoolP224r1	224
12	NIST P-256(secp256r1)	256
13	BrainpoolP256r1	256
14	BrainpoolP320r1	320
15	NIST P-384(secp384r1)	384
16	BrainpoolP384r1	384
17	BrainpoolP512r1	512

FCS_CKM.1/CA Cryptographic key generation - Diffie-Hellman for Chip Authentication session keys

15) *[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111]*
16) *[assignment: cryptographic key sizes]*
17) *[selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH* compliant *to BSI TR-03111]*
18) *[assignment: cryptographic key sizes]*
19) *[assignment: list of standards]*

162 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: 1. <*Diffie-Hellman*>[20] and specified cryptographic key sizes: <*2048*>[21], that meet the following: <based on the Diffie-Hellman key derivation protocol compliant to **[RSA-PKCS#3]** and **[EAC-TR]**>[22], or 2. <*ECDH*>[23] and specified cryptographic key sizes: <*192, 224, 256, 384, 512*>[24], that meet the following: <based on an ECDH protocol compliant to **[ECC-TR]**>[25].

Application Note 31 : FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [EAC-TR].

Application Note 32 : The TOE generates a shared secret value with the terminal during the Chip Authentication protocol Version 1, see [EAC-TR]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [RSA-PKCS#3]) or on the ECDH compliant to TR-03111 [ECC-TR] (i.e. the elliptic curve cryptographic algorithm - cf. [ECC-TR] 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 [EAC-TR]).

Application Note 33 : The TOE implements the hash function SHA-1 according to [EACPassPP] AN 14 and uses SHA-2 according to [EAC-TR] for EAC-TA.

Application Note 34 : Chip Authentication session keys are not generated if PACE-CAM has been performed, as in this case Chip Authentication protocol version 1 is skipped.

20) [assignment: cryptographic key generation algorithm]
21) [assignment: cryptographic key sizes]
22) [assignment: list of standards]
23) [assignment: cryptographic key generation algorithm]
24) [assignment: cryptographic key sizes]
25) [assignment: list of standards]

Application Note 35 : If PACE Chip Authentication Mapping is performed, the Secure Messaging session established by the PACE protocol is sustained. In this case FCS_CKM.1/DH_PACE applies instead of FCS_CKM.1/CA.

FCS_CKM.1/PAC Cryptographic key generation − Generation of PAC session keys

163 Hierarchical to: No other components.

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

FCS_CKM.1.1/PAC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm : <*TDES or AES key derivation*>26) and specified cryptographic key sizes: <*112 ,128*>27), that meet the following: <*[ICAO-9303] Part-11 9.7 Key Derivation Mechanism*>28)

Application Note 36 : 3-DES is also supported by the TOE for PAC authentication mechanism, but this is not considered in the scope of this ST in accordance with Application note 31 in [BACPassPP]

164 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (CC part 2).

FCS_CKM.4 Cryptographic key destruction − Session keys

165 Hierarchical to: No other components.

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

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: <*physical deletion by overwriting the*

26) [assignment: cryptographic key generation algorithm]
27) [assignment: cryptographic key sizes]
28) [assignment: list of standards]
29) [assignment: cryptographic key destruction method]

	memory data with zeros or the new key>[29] that meets the following: <*none*>[30]

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. And, Concerning the PAC keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/PAC.

166 The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (CC part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/AA_SIGN Cryptographic operation − Signature for Active Autentication

167 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 for Active Authentication data*>[31] in accordance with a specific cryptographic algorithm: 1. <*RSA*>[32] and specified cryptographic key sizes: <*2048*>[33], that meet the following: <*[ISO 9796-2]*>[34], or 2. <*ECDSA*>[35] and specified cryptographic key sizes: <*224,256,384,512*>[36], that

30) *[assignment: list of standards]*
31) *[assignment: list of cryptographic operations]*

	meet the following: <[ECC-TR]>37),

Application Note 38 : 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-9303].

FCS_COP.1/PACE_ENC Cryptographic operation − Encryption/Decryption AES/3-DES

168 Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4

FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption[38] in accordance with a specified cryptographic algorithm <AES and 3-DES in CBC mode>[39] and cryptographic key sizes <112 (for 3-DES), and 128, 192 and 256 bit (for AES)>[40] that meet the following: compliant to **[ICAO-9303]**[41].

Application Note 39 : This SFR requires the TOE to implement the cryptographic primitive AES or 3-DES 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).

FCS_COP.1/PACE_MAC Cryptographic operation − MAC

169 Hierarchical to: No other components.

32) [assignment: cryptographic key generation algorithm]
33) [assignment: cryptographic key sizes]
34) [assignment: list of standards]
35) [assignment: cryptographic key generation algorithm]
36) [assignment: cryptographic key sizes]
37) [assignment: list of standards]
38) [assignment: list of cryptographic operations]
39) [selection: AES, 3DES] in CBC mode
40) [selection: 112, 128, 192, 256]
41) [assignment: list of standards]

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

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

FCS_CKM.1 Cryptographic key generation]: fulfilled by

FCS_CKM.1/DH_PACE

FCS_CKM.4 Cryptographic key destruction : fulfilled by FCS_CKM.4

FCS_COP.1.1/ PACE_MAC	The TSF shall perform secure messaging – message authentication code[42] in accordance with a specified cryptographic algorithm <CMAC and Retail MAC>[43] and cryptographic key sizes <112, 128, 192 and 256 bit>[44] that meet the following: compliant to **[ICAO-9303]**[45]

Application Note 40 : This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with [ICAO-9303] the (two-key) 3-DES could be used in Retail mode for secure messaging.

FCS_COP.1/CA_ENC Cryptographic operation − Symmetric Encryption/Decryption

170 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[46] in accordance with a specified cryptographic algorithm <*AES and 3-DES*>[47] and cryptographic key sizes <*112 (for 3-DES) and 128, 192 and 256 bit (for AES)*>[48] that meet the following: <*compliant to [ICAO-9303] and [EAC-TR]*>[49].

42) [assignment: list of cryptographic operations]
43) [selection: CMAC, Retail-MAC]
44) [selection: 112, 128, 192, 256]
45) [assignment: list of standards]
46) [assignment: list of cryptographic operations]
47) [assignment: cryptographic algorithm]
48) [assignment: cryptographic key sizes]
49) [assignment: list of standards]

Application Note 41 : This SFR requires the TOE to implement the cryptographic primitives (e.g. 3-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.

FCS_COP.1/CA_MAC Cryptographic operation – MAC

171 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[50] in accordance with a specified cryptographic algorithm <*CMAC and Retail MAC*>[51] and cryptographic key sizes <*112, 128, 192 and 256 bit*>[52] that meet the following: <*compliant to [ICAO-9303] and [EAC-TR]*[53].

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.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document

172 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[54] in accordance with a

50) *[assignment: list of cryptographic operations]*
51) *[assignment: cryptographic algorithm]*
52) *[assignment: cryptographic key sizes]*
53) *[assignment: list of standards]*

	specified cryptographic algorithm 1. <*RSA as specified in Table 6-4*>[55] and cryptographic key sizes: <*2048 bit*>[56] that meet the following: <*[RSA-PKCS#1]*>[57] or 2. <*ECDSA with plain signature format as specified in Table 6-5*>[58] and cryptographic key sizes: <*192, 224, 256, 384 and 512 bit*>[59] that meet the following: <*[EAC-TR]*>[60].

(Table 6-4) RSA algorithms for signature verification in Terminal Authentication ([EAC-TR])

Object Identifier	Signature	Hash	Parameters
id-TA-RSA-v1-5-SHA-256	RSASSA-PKCS1-v1_5	SHA-256	N/A
id-TA-RSA-v1-5-SHA-512	RSASSA-PKCS1-v1_5	SHA-512	N/A
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

(Table 6-5) ECDSA algorithms for signature verification in Terminal Authentication ([EAC-TR])

Object Identifier	Signature	Hash
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256
id-TA-ECDSA-SHA-384	ECDSA	SHA-384
id-TA-ECDSA-SHA-512	ECDSA	SHA-512

Application Note 43 : 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.

54) [assignment: list of cryptographic operations]
55) [assignment: cryptographic algorithm]
56) [assignment: cryptographic key sizes]
57) [assignment: list of standards]
58) [assignment: list of cryptographic operations]
59) [assignment: cryptographic key sizes]
60) [assignment: list of standards]

FCS_COP.1/PAC Cryptographic operation − Symmetric encryption/decryption and MAC during Personalization

173 Hierarchical to : No other components.

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

FCS_COP.1.1/PAC	The TSF shall perform <*symmetric encryption and decryption*>[61] in accordance with a specified cryptographic algorithm <*3-DES, AES*>[62] and cryptographic key sizes <*112, 128 bit*>[63] that meet the following : <*Table 6-6*>[64]

(Table 6-6) Algorithms and key sizes for PAC

Algorithm	Key size	List of standards
TDES encryption and decryption	112 bits	[SP 800-67]
AES encryption and decryption	128 bits	[FIPS 197]
TDES Retail MAC	112 bits	[ISO 9797]
AES CMAC	128 bits	[NIST-SP800-38B]

Application Note 44 : TDES is also supported by the TOE for PAC security mechnism(PAC authentication mechanism), but his is not considered in the scope of this ST in accordance with Application note 31 in [BACPassPP]

174 The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (CC part 2 extended).

FCS_RND.1 Quality metric for random numbers

175 Hierarchical to: No other components.

Dependencies: No dependencies.

61) *[assignment: list of cryptographic operations]*
62) *[selection: AES, 3DES] in CBC mode*
63) *[selection: 112, 128]*
64) *[assignment: list of standards]*

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet <*BSI AIS-31 functionality class PTG.2 of German scheme and RGS of French scheme [DTRNG]*>[65].

Application Note 45 : This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols as required by FIA_UAU.4/PACE.

6.1.3. Class FIA Identification and Authentication

176 The following Table provides an overview of the authentication mechanisms used.

(Table 6-7) Overview of authentication SFRs

Mechanism	SFR for the TOE
Authentication Mechanism for Personalization Agents	FIA_UAU.4/PACE FIA_UAU.1/PAC FIA_AFL.1/PAC
Chip Authentication Protocol v.1	FIA_API.1/CA FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE FIA_AFL.1/TA
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication	FIA_API.1/AA

Application Note 46 : the Chip Authentication Protocol Version 1 as defined in this security target includes

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

65) *[assignment: a defined quality metric]*

with the expected key for any message received by the terminal.

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

Application Note 47 : If PACE Chip Authentication Mapping is used, the secure messaging keys established by the PACE protocol are sustained. A subsequent Terminal Authentication Protocol v.1 uses the PACE-CAM public key verified during the PACE protocol.

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

FIA_AFL.1/PAC Authentication failure handling in Pesonalization

178 Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication:fulfilled by FIA_UAU.1/PAC

FIA_AFL.1.1/PAC	The TSF shall detect when <*5*>66) unsuccessful authentication attempts occur related to <*consecutive failed authentication attempts with respect to the initialization key*>67).
FIA_AFL.1.2/PAC	When the defined number of consecutive unsuccessful authentication attempts has been <met>68), the TSF shall <*block the Personalization key and terminate TOE*>69).

FIA_AFL.1/PACE Authentication failure handling − PACE authentication using non-blocking authorization data

179 Hierarchical to: No other components.

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

FIA_AFL.1.1/PACE	The TSF shall detect when <*2*>70) unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password 71).

66)[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
67) [assignment: list of authentication events]
68) [selection: met, surpassed]
69) [assignment: list of actions]

FIA_AFL.1.2/PACE	When the defined number of consecutive unsuccessful authentication attempts has been met[72], the TSF shall <*delay the next authentication attempt at least 10 seconds*>[73].

Application Note 48 : Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy, 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 requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of this ST. One of some opportunities for performing this operation might be 'consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'.

FIA_AFL.1/TA Authentication failure handling in Terminal Authentication

180 Hierarchical to: No other components.

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

FIA_AFL.1.1/TA	The TSF shall detect when <*1*>[74] unsuccessful authentication attempts occur related to <*authentication failure of terminal authentication*>[75].
FIA_AFL.1.2/TA	When the defined number of consecutive unsuccessful authentication attempts has been <met>[76], the TSF shall <*retains Secure Messaging(unless a Secure Messaging error occures) and removes remaining information related to Terminal Authentication*>[77].

181 The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (CC part 2).

FIA_UID.1/PAC Timing of identification

182 Hierarchical to: No other components.

---

70) [assignment: positive integer number]
71) [assignment: list of authentication events]
72) [assignment: met or surpassed]
73) [assignment: list of actions]
74)[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
75) [assignment: list of authentication events]
76) [selection: met, surpassed]
77) [assignment: list of actions]

Dependencies: No dependencies.

FIA_UID.1.1/PACE	The TSF shall allow 1. <*to establish the communication channel,*> 2. <*carrying out the PAC authentication with PAC authentication key.*> 3. <*to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS.*> 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.

FIA_UID.1/PACE Timing of identification

183 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to **[ICAO-9303]**, 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 **[EAC-TR]** 5. to carry out the Terminal Authentication Protocol v.1 according to **[EAC-TR]**[78] 6. <*to carry out the Active Authentication Mechanism*>[79] 7. <*to carry out the PACE Chip Authentication Mapping Protocol according to [ICAO-9303]*>[80] 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 49 : The SFR FIA_UID.1/PACE covers the definition in PACE PP [PACEPassPP] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

78) *[assignment: list of TSF-mediated actions]*
79) *[assignment: list of TSF-mediated actions]*
80) *[assignment: list of TSF-mediated actions]*

Application Note 50 : 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-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 “Personalisation of the travel document”. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation 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 Personalisation Agent (using the Personalisation Agent Key).

Application Note 51 : User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).

Application Note 52 : In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC. Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents(refer to FIA_UID.1/PAC, FIA_UAU.1/PAC). 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 ‘Personalisation Agent’, when a terminal proves the respective Terminal authorisation Level as defined by the related policy (policies).

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

FIA_UAU.1/PAC Timing of authentication

185 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfulled by FIA_UID.1/PAC

FIA_UAU.1.1/PACE	The TSF shall allow 1. <*to establish the communication channel,*> 2. <*carrying out the PAC authentication with PAC authentication key.*> 3. <*to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS.*> on behalf of the user to be performed before the user is identified.
FIA_UAU.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.

FIA_UAU.1/PACE Timing of authentication

186 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to **[ICAO-9303],** 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to identify themselves by selection of the authentication key 5. to carry out the Chip Authentication Protocol v.1 according to **[EAC-TR]**, 6. to carry out the Terminal Authentication Protocol v.1 according to **[EAC-TR]**[81], 7. <*to carry out the Active Authentication Mechanism*>[82] 8. <*to carry out the PACE Chip Authentication Mapping Protocol according to [ICAO-9303]*>[83] on behalf of the user to be performed before the user is identified.
FIA_UAU.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 53 : The SFR FIA_UAU.1/PACE in EAC PP covers the definition in PACE PP [PACEPassPP] and extends it by EAC aspect 5. This extension does not conflict with the

81) *[assignment: list of TSF-mediated actions]*
82) *[assignment: list of TSF-mediated actions]*
83) *[assignment: list of TSF-mediated actions]*

strict conformance to PACE PP.

Application Note 54 : The user authenticated after a successfully performed PACE proto-col is a terminal. If PACE was successfully performed, Secure Messaging is started us-ing the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

Application Note 55 : The user authenticated after a successfully performed TA protocol is a Service Provider represented by Extended Inspection System.

187 The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (CC part 2).

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

188 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according to **[ICAO-9303],** 2. Authentication Mechanisms based on <AES, 3-DES>[84]**,** 3. Terminal Authentication Protocol v.1 according to **[EAC-TR]**[85].

Application Note 56 : The SFR FIA_UAU.4.1 covers the definition in PACE PP [PACEPassPP] 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 [EACPassPP].

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. And also, TOE provides the function for preventing reuse of random data during PAC authentication with Personalization Agent.

84) [selecion: Triple-DES, AES or other approved algorithms]
85) [assignment: identified authentication mechanism(s)]

189 The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (CC part 2).

FIA_UAU.5/PACE Multiple authentication mechanisms

190 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE	The TSF shall provide 1. PACE Protocol according to **[ICAO-9303]**, 2. Passive Authentication according to **[ICAO-9303],** 3. Secure messaging in MAC-ENC mode according to **[[ICAO-9303],** 4. Symmetric Authentication Mechanisms based on <3-DES, AES>[86] 5. Terminal Authentication Protocol v.1 according to **[EAC-TR]**[87] 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 <Symmetric Authentication Mechanism based on AES with Personalization Agent key>[88]. 3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1 4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1[89] 5. <*If PACE Chip Authentication Mapping has been performed instead of Chip Authentication Protocol Version 1 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 PACE Chip Authentication Mapping and the secure messaging established by the PACE Protocol>[90].

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

Application Note 59 : Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of ePassport application.

191 The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (CC part 2)

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

192 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[91].

Application Note 60 : The PACE protocol specified in [ICAO-9303] 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

86) [selection: Triple-DES, AES or other approved algorithms
87) [assignment: list of multiple authentication mechanism(s)]
88) [selection: the Authentication Mechanism with Personalization keys]
89) [assignment: rules describing how the multiple authentication mechanisms provide authentication]
90) [assignment: rules describing how the multiple authentication mechanisms provide authentication]
91) [assignment: list of conditions under which re-authentication is required]

from the initially authenticated terminal.

Application Note 61 : The SFR FIA_UAU.6/PACE also includes PACE Chip Authentication Mapping.

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

193 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC/CAV1	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[92].

Application Note 62 : The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO-9303], include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

194 The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (CC part 2 extended).

FIA_API.1/CA Authentication Proof of Identity

195 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CAV1	The TSF shall provide a Chip Authentication Protocol Version 1 according to **[EAC-TR]**[93] to prove the identity of the TOE[94]

92) [assignment: list of conditions under which re-authentication is required]
93) [assignment: authentication mechanism]
94) [assignment: authorized user or rule]

Application Note 63: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [EAC-TR]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303]. 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 by Active Authentication

196 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA	The TSF shall provide a <*Active Authentication Protocol according to [ICAO-9303]*[95)]> to prove the identity of the <*TOE*[96)]>.

Application Note 64 : This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generate a challenge then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corrensponding to the Active Authentication public key (EF.DG.15)

FIA_API.1/PACE-CAM Authentication Proof of Identity by PACE-CAM

197 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA	The TSF shall provide a <*Chip Autnetication Mapping according to [ICAO-9303]*[97)]> to prove the identity of the <*TOE*[98)]>.

Application Note 65 : This SFR requires the TOE to implement the Chip Authentication as either part of PACE-CAM specified in [ICAO-9303]. In the case of PACE-CAM the terminal verifies the authenticity of the chip using the Chip Authentication Data sent by the travel-document.

198 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below

95) [assignment: authentication mechanism]
96) [assignment: authorized user or rule]
97) [assignment: authentication mechanism]
98) [assignment: authorized user or rule]

(Common Criteria part 2).

FDP_ACC.1/TRM Subset access control

199 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[99] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document[100]

Application Note 66 : The SFR FIA_ACC.1.1 covers the definition in [PACEPassPP] and extends it by data stored in EF.SOD of the logical travel document. This extension does not conflict with the strict conformance to [PACEPassPP].

200 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (CC part 2).

FDP_ACF.1/TRM Security attribute based access control − Terminal Access

201 Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM

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, d. <*Personalization Agent*> **2.** Objects: a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD, EF.COM, **EF.CVCA, EF.CardAccess and EF.CardSecurity** of

99) *[assignment: access control SFP]*
100) *[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]*
101) *[e.g. Chip Authentication Version 1 and ephemeral keys]*

	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[101] **3.** Security attributes: a. PACE Authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal[102]. d. <*PAC Authentication*>
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: 1. <*the successfully authenticated Personalization Agent is allowed to write and to read data objects from FDP_ACF.1.1/TRM according to [ICAO-9303]*> 2. BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to **[ICAO-9303]** after a successful PACE authentication as required by FIA_UAU.1/PACE[103].
FDP_ACF.1.3/TRM	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[104]
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[105].

Application Note 67 : The SFR FDP_ACF.1.1/TRM covers the definition in [PACEPassPP] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM cover the definition in [PACEPassPP]. The SFR FDP_ACF.1.4/TRM covers the definition in [PACEPassPP] and extends it by 3) to 6). These extensions do not conflict with the strict conformance to [PACEPassPP].

Application Note 68 : The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [EAC-TR] . 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 69 : Please note that the Document Security Object (SOD) stored in EF.SOD (see [ICAO-9303]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [ICAO-9303].

Application Note 70 : Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

102) [assignment: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
103) [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
104) [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
105) [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

Application Note 71 : 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).

202 The TOE shall meet the requirement "Subset residual information protection" (FDP_RIP.1) as specified below (CC part 2).

FDP_RIP.1 Subset residual information protection

203 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>[106] the following objects. 1. Session Keys (immediately after closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K), 3. <*PAC key (after the end of personalization phase and switching to Discard)*>[107].

Application note 72 : 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.

204 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (CC part 2).

106) *[selection: allocation of the resource to, deallocation of the resource from]*
107) *[assignement:list of objects]*

FDP_UCT.1/TRM Basic data exchange confidentiality - travel-document

205 Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]: fulfilled by FTP_ITC.1/PACE

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM

FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP[108] to be able to transmit and receive[109] user data in a manner protected from unauthorized disclosure.

206 The TOE shall meet the requirement "Basic data exchange integrity (FDP_UIT.1)" as specified below (CC part 2).

FDP_UIT.1/TRM Data exchange integrity

207 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]: fulfilled by FDP_ACC.1/TRM

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]: fulfilled by FTP_ITC.1/PACE

FDP_UIT.1.1/TRM	The TSF shall enforce the Access Control SFP[110] to be able to transmit and receive[111] user data in a manner protected from modification, deletion, insertion and replay[112] errors
FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[113] has occurred.

Application Note 73 : 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

108) [assignment: access control SFP(s) and/or information flow control SFP(s)]
109) [selection: transmit, receive]
110) [assignment: access control SFP(s) and/or information flow control SFP(s)]
111) [selection: transmit, receive]
112) [selection: modification, deletion, insertion, replay]
113) [selection: modification, deletion, insertion, replay]

message authentication codes after successful PACE, successful PACE-CAM or successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.1.5 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE or Chip Authentication

208 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[114)]

Application Note 74 : 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 75 : The trusted channel is established after successful performing the Chip Authentication protocol or the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}); If the Chip Authentication protocol was successfully performed, secure messaging is immediately restarted using the derived session keys. This secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE. Note that Terminal Authentication also requires secure messaging with the

114) [assignment: list of functions for which a trusted channel is required] session keys established after either Chip Authentication as part of PACE-CAM or as Chip Authentication Protocol Version 1.

Application Note 76 : Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.1.4. Class FMT Security Management

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

210 The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (CC part 2).

FMT_SMF.1 Specification of Management Functions

211 Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-Personalization, 3. Personalization, 4. Configuration[115].

212 The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (CC part 2).

FMT_SMR.1/PACE Security roles

213 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	The TSF shall maintain the roles:

115) [assignment: list of security management functions to be provided by the TSF]

	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	The TSF shall be able to associate users with roles.

Application Note 77 : The SFR FMT_SMR.1.1/PACE in the current ST covers the definition in [PACEPassPP] and extends it by 5) to 8). This extension does not con-flict with the strict conformance to [PACEPassPP].

214 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below(CC part 2 extended).

Application Note 78 : The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

FMT_LIM.1 Limited capabilities

215 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 disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and

	5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[116].

6.1.6.4 FMT_LIM.2 Limited availability

216 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (CC part 2 extended).

FMT_LIM.2 Limited availability

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

Application Note 79 : 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.

Application Note 80 : Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application Note 81 : 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.

116) [assignment: limited capability and availability policy]

218 The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (CC part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data − Writing of Initialization Data and Prepersonalization Data

219 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions; fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write[117] the Initialization Data and Pre-personalization Data[118] to the Manufacturer[119].

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

220 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to read out[120] the Initialization Data and the Pre-personalization Data[121] to the Personalization Agent[122]

Application Note 82 : The TOE may restrict the ability to write the Initialization 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 Initialization 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 phases 'manu-facturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, the read and use access shall be blocked in the 'operational use' by the Personalization Agent, when he switches the TOE from the life phase 'issuing' to the life phase 'operational use'.

117) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
118) [assignment: list of TSF data]
119) [assignment: the authorised identified roles]
120) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
121) [assignment: list of TSF data]
122) [assignment: the authorised identified roles]

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

221 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[123] 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*>[124]

Application Note 83 : The initial Country Verifying Certification Authority Public Key may be written by the Personalization Agent (cf. [EAC-TR]). 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

222 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[125] the: 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate[126], to Country Verifying Certification Authority[127]

Application Note 84 : The Country Verifying Certification Authority updates its asymmetric

123) *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
124) *[assignment: the authorized identified roles]*
125) *[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*
126) *[assignment: list of TSF data]*
127) *[assignment: the authorised identified roles]*

key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [EAC-TR]). 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. [EAC-TR]).

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

223 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[128] the Current Date[129] to: 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System[130]

Application Note 85 : The authorized roles are identified in their certificate (cf. [EAC-TR]). and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. [EAC-TR]).

FMT_MTD.1/PAC_KEY Management of TSF data − Updating of PAC Key

224 Hierarchical to: No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/PAC_KEY	The TSF shall restrict the ability to <*modify*>[131] the <*PAC Authentication key*>[132] to the <*Personalization Agent*>[133]

FMT_MTD.1/PACE_CAMPK Management of TSF data − PACE Chip Authentication

128) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
129) [assignment: list of TSF data]
130) [assignment: the authorised identified roles]
131) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
132) [assignment: list of TSF data]
133) [assignment: the authorised identified roles]

Mapping Private Key

225 Hierarchical to: No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/PACE_CAMPK	The TSF shall restrict the ability to <*load*>[134] the <*PACE Chip Authentication Mapping Private Key*>[135] to the <*Personalization Agent*>[136]

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

226 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>[137] the Chip Authentication Private Key[138] to <*the Personalization Agent*>[139]

Application Note 86 : The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. This operation is no more available after Personalization.

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

227 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to <load>[140] the <*Active Authentication Private Key*>[141] to the <*Personalization Agent*>[142]

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

134) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
135) [assignment: list of TSF data]
136) [assignment: the authorised identified roles]
137) [selection: create, load]
138) [assignment: list of TSF data]
139) [assigned: the authorised identified roles]
140) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
141) [assignment: list of TSF data]
142) [assignment: the authorised identified roles]

228 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[143]: 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalization Agent Keys, 4. <*Active Authentication Private Key*>[144] 5. <*PACE Chip Authentication Mapping Private Key*>[145] to none[146].

Application Note 87 : The SFR FMT_MTD.1/KEY_READ in this ST covers the definition in the EAC PP [EACPassPP] that, in turn, extends the definition in PACE PP [PACEPassPP] 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

229 Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/PA	The TSF shall restrict the ability to write[147] the Document Security Object (SOD)[148] to the Personalization Agent[149].

Application Note 88 : 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.

230 The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (CC part 2).

143) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
144) [assignment: list of TSF data]
145) [assignment: list of TSF data]
146) [assignment: the authorised identified roles]
147) [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
148) [assignment: list of TSF data]
149) [assignment: the authorised identified roles]

FMT_MTD.3 Secure TSF data

231 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[150].

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

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE and the expiration date of 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 89 : The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.5. Class FPT Protection of the Security Functions

232 The TOE shall prevent inherent and forced illicit information leakage for User Data and

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

TSFdata.The security functional requirement FPT_EMS.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE security functionality.

233 The TOE shall meet the requirement “TOE emanation (FPT_EMS.1)” as specified below (CC part 2 extended):

FPT_EMS.1 TOE Emanation

234 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1	The TOE shall not emit <*power variations, timing variations during command execution*>[151] in excess of <*non-useful information*>[152] enabling access to 1. Chip Authentication session Keys, 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. <*PAC Session Keys*>[153] 5. Personalization Agent Keys, 6. Chip Authentication Private Key, 7. <*Active Authentication Private Key*>[154], 8. <*PACE Chip Authentication Mapping Private Key*>[155]
FPT_EMS.1.2	The TSF shall ensure any users[156] are unable to use the following interface smart card circuits contacts[157] to gain access to 1. Chip Authentication session Keys, 2. PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. <*PAC Session Keys*>[158]

	5. Personalization Agent Keys, 6. Chip Authentication Private Key, 7. <*Active Authentication Private Key*>[159], 8. <*PACE Chip Authentication Mapping Private Key*>[160]

Application Note 90 : The SFR FPT_EMS.1.1 covers the definition given in the Protection Profile [PACEPassPP] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_\EMS.1.2 covers the definition in [PACEPassPP] and extends it by EAC aspects 1., 5. and 6. As claimed in [EACPassPP] these extensions do not conflict with the strict conformance to [PACEPassPP].

Application Note 91 : The TOE prevents attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contact according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

236 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (CC part 2).

151) [assignment: list of audit information]
152) [assignment: types of emissions]
153) [assignment: list of types of TSF data]
154) [assignment: list of types of user data]
155) [assignment: list of types of user data]
156) [assignment: type of users]
157) [assignment: type of connection]
158) [assignment: list of types of TSF data]
159) [assignment: list of types of user data]
160) [assignment: list of types of user data]

FPT_FLS.1 Failure with preservation of secure state

237 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***>[161]

238 The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (CC part 2).

FPT_TST.1 TSF testing

239 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1	The TSF shall run a suite of self tests <during initial start-up, periodically during normal operation, <*during cryptographic computation and before any use of TSF data*>>[162] to demonstrate the correct operation of the TSF[163].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[164].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[165].

Application Note 92 : During initial start-up RNG live test, it runs sensor test and Fault Attack detection and performs periodically monitoring of Fault Attack detection module and RNG H/W module. It also runs various Fault Attack detection before and after crypto operation and verification of integrity by calculating checksum value before using TSF data strored in protective memory.

161) [assignment: list of types of failures in the TSF]

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

163) [selection: [assignment: parts of TSF], the TSF]

164) [selection: [assignment: parts of TSF], TSF data]

165) [selection: [assignment: parts of TSF], TSF]

Application Note 93 : The travel document's chip uses state of the art smart card technology, therefore it will run the some self tests at the request of an authorized user and some self tests automatically (cf. [HWST]). E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 is executed during initial start-up by the 'authorised user' Manufacturer in the life phase 'Manufacturing'. Other self tests 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 of an integrity check value as soon as data is accessed and to check a calculation with a private key by the reverse calculation with the corresponding public key as a contermeasure against Differentical Faulure Analysis..

240 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (CC part 2).

FPT_PHP.3 Resistance to physical attack

241 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[166)] to the TSF[167)] by responding automatically such that the SFRs are always enforced.

Application Note 94 : 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.

166) [assignment: physical tampering scenarios]
167) [assignment: list of TSF devices/elements]

6.2. Security Assurance Requirements for the TOE

242 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 (Sufficiency of security measures),
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

(Table 6-8) summarizes the assurance components that define the security assurance requirements for the TOE.

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
ADV	AVA_VAN.5

6.3. Security Requirements Rationale

6.3.1. Security functional requirements rationale

(Table 6-9) Coverage of Security Objective for the TOE by SFR

	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 Malfunction
FAU_SAS.1				X				X					
FCS_CKM.1/DH_PACE					X	X	X						
FCS_CKM.1/CA	X	X		X	X	X	X						
FCS_CKM.1/PAC	X			X	X	X	X						
FCS_CKM.4	X			X	X	X	X						
FCS_COP.1/AA_SIGN			X										
FCS_COP.1/PACE_ENC							X						
FCS_COP.1/PACE_MAC					X	X							
FCS_COP.1/CA_ENC	X	X		X	X		X						
FCS_COP.1/CA_MAC	X	X		X	X								
FCS_COP.1/SIG_VER	X			X									
FCS_COP.1/PAC	X			X	X	X	X						
FCS_RND.1	X			X	X	X	X						
FIA_AFL.1/PAC	X			X	X	X	X						
FIA_AFL.1/PACE											X		
FIA_AFL.1/TA	X			X									
FIA_UID.1/PACE	X			X	X	X	X						
FIA_UID.1/PAC	X			X	X	X	X						
FIA_UAU.1/PACE	X			X	X	X	X						
FIA_UAU.1/PAC	X			X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X						
FIA_UAU.5/PACE	X			X	X	X	X						
FIA_UAU.6/PACE					X	X	X						
FIA_UAU.6/EAC	X			X	X	X	X						
FIA_API.1/CA		X											
FIA_API.1/PACE-CAM		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						
FTP_ITC.1/PACE					X	X	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/PAC_Key				X	X								
FMT_MTD.1/PACE_CAMPK		X			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						
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	

243 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 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.

244 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/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the 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.DG13, EF.DG16 of the logical travel-document only once. FMT_MTD.1/PA

covers the related property of OT.AC_Pers (writing SO_D and, in generally, 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, the Chip Authentication Private Key and Active Authentication key. PAC key for authentication between Personalization Agent and TOE can be updated according to SFR FMT_MTD.1/PAC 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, FIA_UID.1/PAC, FIA_UAU.1/PAC, FIA_AFL.1. If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with the Personalization key the TOE will use TSF according to the FCS_RND.1(for the generation of the challenge) and FCS_CKM.1/PAC, FCS_COP.1/PAC (symmetric encryption/decryption and MAC during Presonalization). The session keys are destroyed according to FCS_CKM.4 after use.

If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

245 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 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 SO_D 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. PAC key for authentication between Personalization Agent and TOE can be updated according to SFR FMT_MTD.1/PAC Key.

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_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 K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFRs FIA_UAU.6/EAC, FDP_UIT.1/TRM and FDP_UCT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication Protocol v.1 by means of secure messaging implemented by the cryptographic functions according to 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 SFRs FMT_MTD.1/CAPK, FMT_MTD.1/AAPK, FMT_MTD.1/PACE_CAMPK and FMT_MTD.1/KEY_READ require that the Chip Authentication Key, Active Authentication key and PACE Chip Authentication Mapping Private Key cannot be written unauthorized or read afterwards.

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.

In personalization, the SFR FCS_CKM.1/PAC and FCS_COP.1/PAC ensure the authenticity of data transfers after successful authentication of the personalization agent according to FIA_UID.1/PAC and FIA_UAU.1/PAC with the support of FIA_AFL.1/PAC.

246 The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication or Active 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_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 K_{MAC}).

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 SO_D 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.

In personalization, the SFR FCS_CKM.1/PAC and FCS_COP.1/PAC ensure the authenticity of data transfers after successful authentication of the personalization agent according to FIA_UID.1/PAC and FIA_UAU.1/PAC with the support of FIA_AFL.1/PAC.

247 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_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 K_{ENC}). 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.
In personalization, the SFR FCS_CKM.1/PAC and FCS_COP.1/PAC ensure the confidentiality of data transfers after successful authentication of the personalization agent according to FIA_UID.1/PAC and FIA_UAU.1/PAC with the support of FIA_AFL.1/PAC.

248 The security objective **OT.Sens_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 v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFRs FIA_UAU.6/EAC and FDP_UCT.1/TRM require the confidentiality protection of the transmitted data after Chip Authentication 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 SFRs FIA_UAU.6/EAC and FDP_UCT.1/TRM also require he confidentiality protection of the transmitted data after PAC authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/PAC (Generation of PAC session keys), and FCS_COP.1/PAC(Symmetric encryption/decryption and MAC during Personalization) 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. The SFRs FIA_UID.1/PAC and FIA_UAU.1/PAC, with the support of FIA_AFL.1/PAC, require the identification and authentication of the pre-personalisation agent.

In case of authentication failure, secure messaging is retained except for secure messaging error and removed remaining information related to terminal authentication according to FIA_AFL.1/TA.

249 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 and the Chip Authentication Mapping by FIA_API.1/PACE-CAM proving the identity of the TOE. The Chip Authentication 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 [EAC-TR] requires additional TSF according to 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. PACE-CAM is performed using a TOE internally stored confidentidal private key as required by FMT_MTD.1/PACE_CAMPK and FMT_MTD.1/KEY_READ.

250 The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity by AA" is ensured by the Active Authentication Mechanism [ICAO-9303] 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. This key is confidentially read to the TOE as defined by FMT_MTD.1/KEY_READ. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/AA_SIGN (for the digital signature of Active Authentication data).

251 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.

252 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.

253 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 this ST, since SOD is card-individual) − FTP_ITC.1/PACE.

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

255 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 usersc 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.

6.3.2. Dependency Rationale

256 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.

257 Table 6-9 shows the dependencies between the SFR of the TOE.

(Table 6-10) Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	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/PAC	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/PAC 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_CKM.1/PAC
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 1 for non-satisfied dependencies
FCS_COP.1/PACE_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/DH_PACE Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_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/DH_PACE Fulfilled by FCS_CKM.4
FCS_COP.1/CA_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/CA, Fulfilled by FCS_CKM.4

FCS_COP.1/CA_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/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 Cryptogr. key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4
FCS_COP.1/PAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptogr. key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/PAC, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	
FIA_AFL.1/PAC	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PAC
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/TA	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PAC	No dependencies	
FIA_UID.1/PACE	No dependencies	
FIA_UAU.1/PACE	FIA_UID.1 Timing of identfication	Fulfilled by FIA_UID.1/PACE
FIA_UAU.1/PAC	FIA_UID.1 Timing of identfication	Fulfilled by FIA_UID.1/PAC
FIA_UAU.4/PACE	No dependencies	
FIA_UAU.5/PACE	No dependencies	
FIA_UAU.6/PACE	No dependencies	
FIA_UAU.6/EAC	No dependencies	
FIA_API.1/CA	No dependencies	
FIA_API.1/PACE-CAM	No dependencies	
FIA_API.1/AA	No dependencies	
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 2 for non-satisfied dependencies
FDP_RIP.1	No dependencies	
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 orFDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	
FMT_SMF.1	No dependencies	
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
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/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/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/PAC_KEY	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/PACE_CAMPK	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	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_PHP.3	No dependencies	

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

Justification No. 1 : Since AA doesn't provide for generation or destruction of cryptographic keys, the FCS_CKM.4 doesn't apply

Justification No. 2 : 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.

6.3.3. Security Assurance Requirements Rationale

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

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

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

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

262 The component ALC_DVS.2 has no dependencies.
The component AVA_VAN.5 depends on:

- ADV_ARC.1, Security architectural description
- ADV_FSP.4, Complete functional specification
- ADV_TDS.3, Basic modular design
- ADV_IMP.1, Implementation representation of the TSF

- AGD_OPE.1, Operational user guidance
- AGD_PRE.1, Preparative procedures
- ATE_DPT.1, Testing: basic design

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

6.3.4. Secuirty Requirements − Mutual Support and Internal Consistency

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

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

266 The dependency analysis in section 6.3.2 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 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these "shared" items.

267 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 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

268 Inconsistency between functional and assurance requirements could only arise if there are functional assurance dependencies which are not met, a possibility which has been shown not to arise in section 6.3.2 "Dependency Rationale"and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 SecurityAssurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7. TOE Summary Specification (ASE_TSS.1)

269 The following sections provide a general understanding of how the TOE is implemented. This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

7.1. TOE Security Functions

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

(Table 7-1) TOE Security Feature

Security Feature	Description
SF.IC	IC chip security feature
SF.PAC_AUTH	PAC authentication and creation of PAC session key
SF.SAC_AUTH	SAC(PACE) authentication and creation of SAC(PACE) session key
SF.EACCA_AUTH	EAC-CA authentication
SF.EACTA_AUTH	EAC-TA authentication
SF.ACTIVE_AUTH	AA authentication
SF.SEC_MESSAGE	Secure messaging
SF.ACC_CONTROL	TSF Access control
SF.RELIABILITY	Protection against Physical Manipulation, TSF selftest, Integrity check

7.1.1. SF.IC

271 The TOE uses TSFs provided by IC chip to enforce security. Refer to documents related to IC chip for details of TSF of the IC chip [HWST].

7.1.2. SF.PAC_AUTH

272 This TSF includes the PAC authentication mechanism for Personalization Agent, the PAC authentication mechanism provides authority control of the security role to the Personalization Agent in the personalization phase. It is composed of PAC Initialization, PAC mutual authentication and PAC session key generation.

- **PAC Initialization**

273 During the PAC Initialization, TOE generates key encryption key(KEK), initializes the file table for LDS filesystem. By performing PAC Initialization, the initialization parameters including PAC authentication key are securely loaded to TOE and the state transition from Empty to Unissue has occurred. PAC Initialization can be performed only once and the state transition from Unissue to Empty is irreversible.

- **PAC mutual authentication**

274 TOE and Personalization Agent authenticate mutually each other. Personalization Agent sends the data to the TOE, then TOE authenticates the Personalization Agent by performing a MAC verification and comparison received cryptographic value. Then TOE sends cryptographic value to the Personalization Agent and Personalization Agent can ensure that TOE is the authenticated one by performing a MAC verification and comparison response cryptographic value.

- **PAC session key generation**

275 After successfully PAC mutual authentication, PAC session keys are generated to establish secure communication channel between TOE and Personalization Agent. The User data and TSF data should be personalized to TOE by means of secure messaging with PAC session keys.

7.1.3. SF.SAC_AUTH

276 This TSF implements SAC authentication mechanism. The SAC security mechanism(Supplement Access Control) provides confidentiality and integrity for the personal data of the ePassport holder via secure messaging when controlling access to the personal data of the ePassport holder records in the TOE and transmitting it to the Inspection System with read-rights. This TSF is composed of SAC mutual authentication and SAC(PACE) session key generation. The

standard domain parameter is supported for PACE. TOE supports GM, IM and CAM algorithms for mapping function.

7.1.4. SF.EACCA_AUTH

277 This TSF implements EAC-CA authentication. It includes the ephemeral-static EC Diffie-Hellman key distribution and Diffie-Hellman key distribution protocols which provides the Inspection System with the generation of the EAC session key for a secure communication channel between the TOE and the Inspection System. In personalization phase, EAC-CA private key is written into the TOE's securely protected area and public key is stored into DG14.
If Chip Authentication Mapping(PACE-CAM) as mapping of PACE protocol is performed, this TSF is not performed.

7.1.5. SF.EACTA_AUTH

278 This TSF implements EAC-TA authentication. The EAC-TA is used by the TOE to implement a challenge-response authentication protocol based on the digital signature to authenticate the EAC-supporting Inspection System. After successfully EAC-CA or PACE-CAM, all data is exchanged by means of secure communication with EAC session key or PACE session key.

7.1.6. SF.ACTIVE_AUTH

279 This TSF provides an AA mechanism with which the TOE verifies that the MRTD chip is genuine to the Inspection System by signing the random number transmitted from the Inspection System; the Inspection System verifies the authenticity of the MRTD chip through verification with the signed values. In personalization phase, AA private key is written into the TOE's securely protected area and public key is stored into DG15.

7.1.7. SF.SEC_MESSAGE

280 This TSF provides a secure communication channel to protect the command message(C-APDU) and response message(R-APDU) between the TOE and the Personalization Agent or the Inspection System. The secure communication channel means that between TOE and

Personalization Agent, that between TOE and Inspection System.

7.1.8. SF.ACC_CONTROL

281 This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. The TOE provides access control rules and management functions for the ePassport application data based on security.

7.1.9. SF.RELIABILITY

282 This TSF executes the residual information management, ensures that any information content of the related crypto is made unavailable. It also performs self-test, provides integrity check, preserves the secure protection when case of abnormal operation and provides countermeasure from physical invasion. etc..

8. Reference

8.1. Acronyms

AA	Active Authentication
BAC	Basic Access Control
BIS	Basic Inspection System
CAN	Card Access Number
CBC	Cipher-block Chaining (block cipher mode of operation)
CC	Common Criteria
COM	Common data group of the LDS (ICAO Doc 9303-10)
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO Doc 9303-10)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
IC	Integrated Circuit
IS	Inspection System
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone

N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PACE	Password Authenticated Connection Establishment
PACE-GM	PACE with Generic Mapping
PACE-IM	PACE with Integrated Mapping
PACE-CAM	PACE with Chip Authentication Mapping
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAC	Supplemental Access Control
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOD	Document Security Object
SPA	Simple Power Analysis
ST	Security Target
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TR	Technical Report
VIZ	Visual Inspection Zone

8.2. 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, see [EAC-TR].

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

Agreement This term is used in BSI-CC-PP-0056-V2-2011 [PACEPassPP] in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.

Active Authentication Security mechanism defined in [ICAO-9303] option by which means the travel document''s chip proves and the inspection system verifies the identity and authenticity of the travel document''s chip as part of a genuine travel document issued by a known State of Organization.

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

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

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

Basic Access Control (BAC) Security mechanism defined in [ICAO-9303] by which means the travel document''s chip proves and the basic inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

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

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

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

Biographical data (biodata) The personalized details of the travel document holder appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAO-9303]

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

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

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

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO-9303]

Country Signing CA Certificate (CCSCA) Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the inspection system.

Country Signing Certification Authority (CSCA) An organization enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see.

[ICAO-9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC-TR].

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 [EAC-TR].

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 BSI-CC-PP-0056-V2-2012.

The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO-9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC-TR].

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 [EAC-TR].

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

Document Basic Access Key Derivation Algorithm The [ICAO-9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

PACE passwords Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO-9303].

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 RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document''s chip. It may carry the Document Signer Certificate (CDS). [ICAO-9303]

Document Signer (DS) 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 SignerCertificate (CDS)(CDS), see [EAC-TR] and [ICAO-9303].
This role is usually delegated to a Personalization Agent.

Document Verifier (DV) An organization enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organization / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State''s border police), by - inter alia - issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorized by at least the national CVCA to issue certificates for national terminals, see [EAC-TR].
Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognize a DV as a subject; hence, it merely represents an organizational entity within this ST.
There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer and a foreign CVCA ensuring enforcing the travel document Issuer''s privacy policy).1,2

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

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person''s identity. [ICAO-9303]

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

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

Extended Access Control Security mechanism identified in [ICAO-9303] by which means the travel document''s chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.

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

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait. [ICAO-9303]

Global Interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all travel documents. [ICAO-9303]

IC Dedicated Software Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players.

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

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

The usage of parts of the IC Dedicated Software might be restricted to certain life cycle 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 cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.

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

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person''s document. [ICAO-9303]

Improperly documented person A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else''s travel document or visa; or (d) no travel document or visa, if required. [ICAO-9303]

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

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

Inspection The act of State examining an travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [ICAO-9303].

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

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

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

Issuing Organization Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]

Issuing State The Country issuing the travel document. [ICAO-9303]

Logical Data Structure (LDS) The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the travel document''s chip.

Logical travel document Data of the travel document holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/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 Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303].

Machine readable zone (MRZ) Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1,the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303].

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

Machine-verifiable biometrics feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO-9303]

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

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

The metadata of a CV certificate comprise the following elements:

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

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

- the file structure implementing the LDS [ICAO-9303],
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except the authentication data itself.

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

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

Password Authenticated Connection Establishment (PACE) A communication establishment protocol defined in [ICAO-9303]. 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 ¼). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.

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

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

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

i establishing the identity of the travel document holder for the biographic data in the travel document,

ii enrolling the biometric reference data of the travel document holder,

iii writing a subset of these data on the physical travel document (optical personalization) and storing them in the travel document (electronic personalization) for the travel document holder as defined in [EAC-TR],

iv writing the document details data,

v writing the initial TSF data,

vi signing the Document Security Object defined in [ICAO-9303] (in the role of DS).

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

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

Personalization Data A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the life cycle phase card issuing.

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

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

Receiving State The Country to which the travel document holder is applying for entry; see [ICAO-9303].

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

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

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

Secondary image A repeat image of the holder"s portrait reproduced elsewhere in the document by whatever means; see [ICAO-9303]

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

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

Standard Inspection Procedure A specific order of authentication steps between an travel document and a terminal as required by [ICAO-9303], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.

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

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

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

Travel document Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO-9303] (there “"Machine readable travel document”").

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

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

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

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

TSF data Data created by and for the TOE that might affect the operation of the TOE ([CC]-Part1).

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

User data All data (being not authentication data)

i stored in the context of the ePassport application of the travel document as defined in [ICAO-9303] and

ii being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-9303]).

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]-Part1). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning ([CC]-Part2).

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

8.3. Technical References

[CC]

Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and General Model; Version 3.1, April 2017, CCMB-2017-04-001,
Part 2: Security Functional Requirements; Version 3.1, April 2017, CCMB-2017-04-002,
Part 3: Security Assurance Requirements; Version 3.1, April 2017, CCMB-2017-04-003
Common Methodology for Information Technology Security Evaluation, Evaluation Metho-dology, Version 3.1, April 2017, CCMB-2017-04-004

[EAC-TR]

Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents,
Part 1 - eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 2015,
Part 2 - Protocols for electronic IDentification, Authentication and trust Services (eIDAS), BSI, Version 2.21, 2016-12,
Part 3 - Common Specifications, BSI, Version 2.21, 2016-12

[ICAO-9303]

ICAO Doc 9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 1-12

[ECC-TR]

Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-06

[BACPassPP]

CC Protection Profile Machine Readable Travel Document with “ICAO Application” Basic Access Control, Version 1.10, BSI-CC-PP-0055, Bundesamt füur Sicherheit in der Informa-tionstechnik (BSI), 2009-03-25

[PACEPassPP]

CC Protection Profile: Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP- 0068-V2-2011, 2011-11-02

[EACPassPP]

CC Protection Profile: Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012, Version 1.3.2, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP- 0056-V2-2012, 2012-12-05

[RSA-PKCS#1]

PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.

[SP 800-67]

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2012

[RSA-PKCS#3]

PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.

[FIPS186]

Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07

[RFC5639]

M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[ISO_9796-2]

ISO/IEC 9796-2:2002, Information technology – Security techniques –
Digital signature schemes giving message recovery – Part 2: Integer factorization
based mechanisms, ISO/IEC, 2008-03.

[HWCR]

Certification Report of S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software S3D350A/ S3D300A/ S3D264A/ S3D232A/ S3D200A/ S3K350A ANSSI-CC-2019/01

[HWST]

Security Target of S3D350A/S3D300A/S3D264A/S3D232A/S3D200A/S3K350A/S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, Version 4.1, 25 OCT 2018.

[DTRNG]

S3D350A/S3K1170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note, 2017.10.12., Rev1.6

[FIPS_197]

FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001-11-26.

[ISO_9797]

ISO/IEC 9797:1999, 2002, Information technology —- Security techniques —- Message Authentication Codes (MACs) —- Multipart Standard, ISO/IEC, 1999, 2002.

[NIST_SP800-38B]

NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology, 2005-05.

[ISO 11770-3]

Information technology − Security techniques − Key management − Part 3: Mechanisms using asymmetric techniques, 2015.