HID Global
viale Remo De Feo, 1
80022 Arzano (NA), ITALY

www.hidglobal.com

SOMA-c018 Machine Readable Electronic Document

Security Target

EAC-PACE-AA

Public Version

Common Criteria version 3.1 revision 5
Assurance Level EAL5+

Version	1.0
Date	2020-07-07
Reference	TCLE170097
Classification	PUBLIC

Table of Contents

List of Tables

List of Figures

Abbreviations and notations

Numerical values

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

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

Denoted text

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

Any terms replacing the one used in the PP are printed blue.

Example: e-Document instead of MRTD.

Key words

The words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” are to be interpreted as described in RFC2119 [R25].

1. Introduction

1.1 ST overview

This document is the sanitized version of the document Security Target for SOMA-c018 Machine Readable Electronic Document – ICAO Application – EAC-PACE-AA [R2].

This Security Target (ST) document defines the security objectives and requirements, as well as the scope of the Common Criteria evaluation of SOMA-c018 Machine Readable Electronic Document.

The Target Of Evaluation (TOE) is the integrated circuit chip Samsung S3D350A (rev2) equipped with operating system SOMA-c018 and with e-Document applications, namely an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303 [R22] [R23] [R24].

The TOE adds security features to a document booklet or card, providing machine-assisted identity confirmation and machine-assisted verification of document security.

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

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 7th ed. Part 11 [R23], and Terminal Authentication according to BSI TR-03110 [R13] [R14],
- Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 7th ed. Part 11 [R23], and
- Active Authentication according to ICAO Doc 9303 7th ed. Part 11 [R23].

The TOE also supports Basic Access Control (BAC) compliant with ICAO Doc 9303 [R23], addressed by another ST [R3].

1.2 ST reference

Table 1-1 ST reference

Title	Security Target Lite for SOMA-c018 Machine Readable Electronic Document - EAC-PACE-AA
Version	1.0
Authors	Gianvito TOZZI, Giovanni LICCARDO, Pasquale NOCE, Marco EVANGELISTA
Reference	TCLE170097

1.3 TOE reference

Table 1-2 TOE reference

TOE name	SOMA-c018 Machine Readable Electronic Document - EAC-PACE-AA
TOE version	2
TOE developer	HID Global
TOE identifier	SOMA-c018_2
TOE identification data	53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 38h 5Fh 32h

The TOE is delivered as a chip ready for initialization. It is identified by the following string, which constitutes the TOE identifier:

SOMA-c018_2
(ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 38h 5Fh 32h)

where:

- “SOMA-c018” is the TOE name,
- the underscore character is a separator, and
- “2” is the TOE version number.

The ASCII encoding of the TOE identifier constitutes the TOE identification data, located in the persistent memory of the chip. Instructions for reading these data are provided by the guidance documentation [R4] [R5] [R6] [R7].

1.4 TOE overview

1.4.1 TOE definition

The TOE is the integrated circuit chip of a machine readable e-Document programmed according to the Password Authenticated Connection Establishment mechanism described in the ICAO Doc 9303 7th edition 2015 Part 11 [R23], which means amongst others according to the Logical Data Structure (LDS) defined in [R22], and additionally providing the Extended Access Control according to the ICAO Doc 9303-11 [R23] and BSI TR-03110 [R13] [R14].

The TOE is composed of:

- the circuitry of the dual-interface e-Document's chip Samsung S3D350A (rev2) (see Appendix A),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the smart card operating system SOMA-c018,
- an ICAO application compliant with ICAO Doc 9303 [R22] [R23],
- the associated guidance documentation [R4] [R5] [R6] [R7].

On account of its composite nature, the TOE evaluation builds on the evaluation of the integrated circuit.

The TOE supports wireless communication through the IC contacts exposed to the outside, as well as wireless communication through an antenna connected to the IC. Both the TOE and the antenna are embedded in a paper or plastic substrate, that provides mechanical support and protection.
Once personalized with the data of the legitimate holder and with security data, the e-Document can be inspected by authorized agents.

The TOE is meant for "global interoperability". According to ICAO the term is understood as "*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*".
The TOE is supplied with a file system that contains all the data used in the context of the ICAO application, as described in the Protection Profiles [R11] [R12].

1.4.2 TOE usage and security features for operational use

A State or Organization issues e-Documents to be used by the holder. The user presents an e-Document to the inspection system to prove his or her identity.

Being the TOE a general-purpose e-Document, it supports both the following types of PACE passwords:

- non-secret passwords not deducible from the logical document, at least without a previous PACE authentication, but printed or displayed on the physical document (e.g. MRZ or CAN as in the case of a PACE e-Passport [R23]);
- secret passwords not deducible from either the logical document, at least without a previous PACE authentication, or the physical document.

For the ICAO application, the document holder can control access to his user data by consciously presenting his document to organizations deputed to perform inspection[1].
In the case of a secret PACE password, the document holder can exert further control over access to his data as in addition to his document, he must separately reveal the password in order to authorize inspection.
The document's chip is integrated into a physical (plastic or paper) substrate. The substrate is not part of the TOE. The tying-up of the document's chip to the plastic/paper document is achieved in accordance with physical and organizational security measures being within the scope of the current security target.

The e-Document in context of this security target contains:

i. data elements on the e-Document's chip according to LDS for contactless or contact machine reading.

Additionally, the e-Document may bear:

ii. visual (eye readable) biographical data and portrait of the holder,

iii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ).

The authentication of the presenter[2] is based on:

- the possession of a valid e-Document personalized with the claimed identity as given on the biographical data page, and
- biometrics using the reference data stored in the e-Document.

[1] User authentication with PACE password, such as CAN or MRZ or shared secret, see [R23].
[2] The person presenting the e-Document to the Inspection System.

The Issuing State or Organization ensures the authenticity of the data of genuine e-Documents. The receiving state trusts a genuine e-Document of an Issuing State or Organization.

For this security target, the e-Document is viewed as the unit of:

- the **physical part of the electronic document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the e-Document holder:
  - i. the biographical data on the biographical data page of the data surface,
  - ii. the printed data in the Machine Readable Zone (MRZ),
  - iii. the printed portrait;
- the **logical e-Document** as data of the e-Document holder stored according to the Logical Data Structure [R22] as specified by ICAO on the integrated circuit. It presents machine readable data including (but not limited to) personal data of the e-Document holder:
  - i. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  - ii. the digitized portraits (EF.DG2),
  - iii. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[3],
  - iv. the other data according to LDS (EF.DG5 to EF.DG16),
  - v. the Document Security Object (SO_D),
  - vi. security data objects required for product management.

The Issuing State or Organization implements security features of the e-Document to maintain the authenticity and integrity of the e-Document and its data. The physical part of the e-Document as the e-Document's chip are uniquely identified by the Document Number.

The physical part of the e-Document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the e-Document's chip) and organizational security measures (e.g. control of materials, personalization procedure). These security measures can include the binding of the e-Document's chip to the e-Document.

[3] These biometric reference data are optional according to [R22]. This ST assumes that the issuing State or Organization uses this option and protects these data by means of extended access control.

The logical e-Document delivered by the IC Manufacturer to the Initialization Agent is protected by a mechanism requiring the decryption of a cryptogram by means of AES-256 cryptography, until completion of the initialization process. After completion, the decryption of the cryptogram is no longer possible.

The logical e-Document delivered by the Initialization Agent to the Pre-personalization Agent is protected by a mutual authentication mechanism based on symmetric cryptography with diversified key, until completion of the pre-personalization process. After completion, the authentication keys are disabled.

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

The ICAO defines the baseline required security methods Passive Authentication and the following optional advanced security methods:

- Basic Access Control to the logical e-Document,
- Active Authentication of the e-Document's chip,
- Extended Access Control to and the Data Encryption of sensitive biometrics as an optional security measure in the ICAO Doc 9303-11 [R23], and
- Password Authenticated Connection Establishment [R23].

The Passive Authentication mechanism is performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical e-Document:

i. in integrity by write-only-once access control and by physical means, and
ii. in confidentiality by the Extended Access Control Mechanism.

As BAC is also supported by the TOE, the e-Document has to be evaluated and certified separately. This is due to the fact that [R10] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

The confidentiality by Password Authenticated Access Control (PACE) is a mandatory security feature of the TOE. The e-Document shall strictly conform to the "Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)" [R12]. Note that [R12] considers high attack potential.
The TOE supports PACE with Generic Mapping (PACE-GM) and with Chip Authentication Mapping (PACE-CAM).

For the PACE protocol according to [R23], the following steps shall be performed:

i. The e-Document's chip encrypts a nonce with the shared password, derived from the PACE password (MRZ, CAN or secret password) and transmits the encrypted nonce together with the domain parameters to the terminal.

ii. The terminal recovers the nonce using the shared password. If this password is derived from MRZ or CAN, MRZ data or CAN data are physically read.

iii. The e-Document's chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys 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.

Additionally, for PACE-CAM only, the following steps shall be performed:

v. The e-Document computes Chip Authentication Data, encrypts them, and sends them to the terminal.

vi. The terminal recovers Chip Authentication Data and verifies the authenticity of the chip.

After successful key negotiation, the terminal and the e-Document's chip provide private communication (secure messaging) [R12] [R23].

This security target requires the TOE to implement the Extended Access Control as defined in [R13] [R14], and additionally the Active Authentication as defined in [R23].
The Extended Access Control consists of two parts: (i) the Chip Authentication and (ii) the Terminal Authentication Protocol version 1 (v.1).
The Chip Authentication may be performed as part of the PACE protocol (see steps v. and vi. above), or as a distinct protocol (Chip Authentication Protocol version 1). Both modes are detailed in section 4.4 of ICAO Doc 9303 Part 11 [R23].
The Chip Authentication (i) authenticates the e-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 either PACE-CAM or Chip Authentication Protocol v.1 have been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.
The Active Authentication authenticates the e-Document to the inspection system.

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

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note that the substrate holding the chip as well as the antenna (if any) and the card are needed to represent a complete e-Document, nevertheless these parts are not essential for the secure operation of the TOE.

1.5 TOE life cycle

The TOE life cycle is comprised of four life cycle phases, i.e. *development*, *manufacturing*, *personalization*, and *operational use*. These phases can be split into eight steps as follows:

1. Phase 1: Development comprises:

   Step 1: the development of the operating system software by the Embedded Software Developer, and

   Step 2: the development of the integrated circuit by the IC Manufacturer;

2. Phase 2: Manufacturing comprises:

   Step 3: the fabrication of the integrated circuit by the IC Manufacturer,

   Step 4: the embedding of the chip in a substrate with an antenna. The antenna may be omitted if the IC contacts are exposed,

   Step 5: the initialization and OS configuration, and

   Step 6: the pre-personalization of the e-Document;

3. Phase 3: Personalization comprises:

   Step 7: the personalization of the e-Document for the holder;

4. Phase 4: Operational use comprises:

   Step 8: the inspection of the e-Document.

Application Note 1 *The entire development phase, as well as step 3, "Manufacture of the IC", of the manufacturing phase are the only phases covered by assurance, as during these phases the TOE is under construction in a protected environment.*

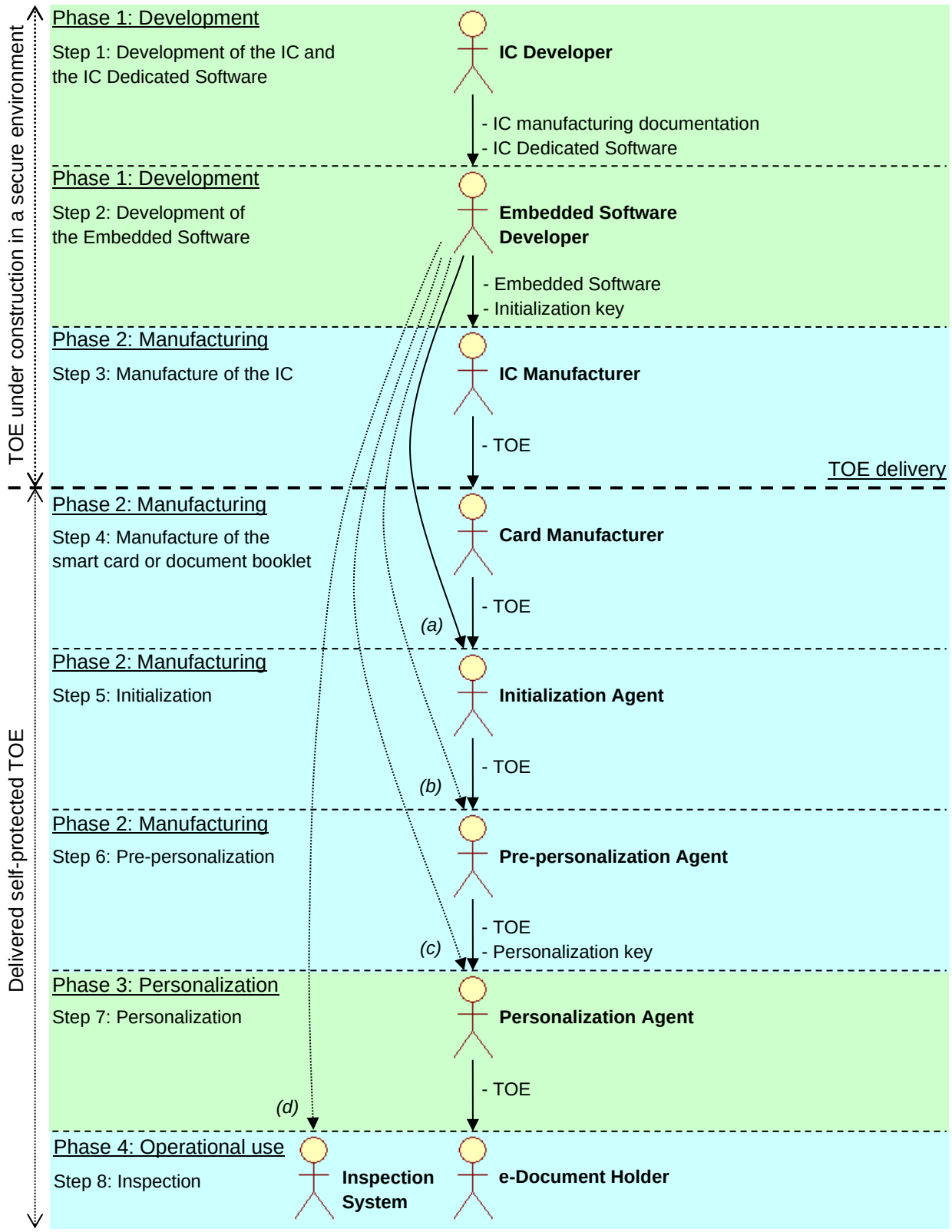
Figure 1-1 represents the life cycle of the TOE. Particularly, it identifies the actors involved in each step of the life cycle. Direct deliveries of items between actors are represented with continuous lines, while deliveries in which intermediate actors may be in charge of receiving

the exchanged items and forwarding them to the subsequent actors are represented with dotted lines.
Deliveries of items occurring between non-consecutive actors are just marked with letters in order to preserve the clarity of the diagram. A legend for these deliveries, which identifies the exchanged items for each of them, is provided in Table 1-3.

Table 1-3 Legend for deliveries occurring between non-consecutive actors

Delivery	Delivered items
(a)	• Initialization cryptograms • Initialization guidance
(b)	• Pre-personalization key • Pre-personalization guidance
(c)	• Personalization guidance
(d)	• Operational user guidance

Figure 1-1 Life cycle of the TOE



Detailed information about the operations available in each life cycle phase of the TOE is provided in the guidance documentation.
Table 1-4 describes the roles taking part in each phase of the life cycle of the TOE. Some roles, printed in italics, collectively identify multiple agents.

Table 1-4 Roles involved in the life cycle of the TOE

Phase	Role	Description	Loaded data
1	IC Developer	Samsung	None
1	Embedded Software Developer	HID Global	None
2	IC Manufacturer	Samsung	Initialization key Pre-personalization key Configuration data Product information
2	Card Manufacturer	The agent who is acting on behalf of the issuing state or organization to assemble the booklet or plastic card by embedding the TOE and antenna into the substrate.	None
2	Initialization Agent	The agent who is acting on behalf of the issuing state or organization to configure the OS and load the pre-personalization key.	Pre-personalization key Configuration data Product information
2	Pre-personalization Agent	The agent who is acting on behalf of the issuing state or organization to pre-personalize the e-Document.	Personalization keys, Chip Authentication keys, Active Authentication keys, Initial LDS configuration, Further details are provided by the Pre-personalization Guidance [R5]
2	*Manufacturer*	Role that collectively identifies all the agents acting in phase 2, namely: • the IC Manufacturer, • the Card Manufacturer, • the Initialization Agent, • the Pre-personalization Agent.	Cf. the rows related to the collected roles
3	Personalization Agent	The agent who is acting on behalf of the issuing state or organization to personalize the e-Document for	ICAO PACE key, Further details are provided by the Pre-

		the holder.	personalization Guidance [R6]
4	e-Document Holder	The rightful owner of the e-Document.	None
4	Inspection System	A technical system used by the control officer of the receiving state or organization (i) to examine an e-Document presented by the holder and verify its authenticity and (ii) to verify the holder as e-Document Holder.	In case of updates of the TA trust point or the chip current date: • TA trust point, • TA trust point CHA, • CVCA, or/and • Chip current date.

Table 1-5 identifies, for each guidance document, the actors who are the intended recipients of that item.

Table 1-5 Identification of recipient actors for the guidance documentation of the TOE

Guidance document	Recipient actors
Initialization guidance	Initialization Agent
Pre-personalization guidance	Pre-personalization Agent
Personalization guidance	Personalization Agent
Operational user guidance	Inspection System

The phases and steps of the TOE life cycle are described in what follows. The names of the involved actors are emphasized using boldface.

1.5.1 Phase 1: Development

Step 1: Development of the IC and the IC Dedicated Software

The **IC Developer** develops the integrated circuit, the IC Dedicated Software, and the guidance documentation associated with these TOE components.

Finally, the following items are securely delivered to the **Embedded Software Developer** and the **IC Manufacturer**:

- the IC manufacturing documentation,
- the IC Dedicated Software.

Step 2: Development of the Embedded Software

The **Embedded Software Developer** uses the guidance documentation for the integrated circuit and for relevant parts of the IC Dedicated Software and develops the Embedded Software, consisting of the OS and the ICAO application, as well as the guidance documentation associated with these TOE components.

Furthermore, the **Embedded Software Developer** generates the initialization key and the pre-personalization key.

Finally:

- the Embedded Software and the initialization key are securely delivered to the **IC Manufacturer**;
- the cryptograms enciphered using the initialization key are securely delivered to the **Initialization Agent**;
- the pre-personalization key is securely delivered to either the **Initialization Agent** or the **Pre-personalization Agent**.

As regards TOE guidance documentation, either all documents are securely delivered to the **Initialization Agent**, or each document is securely delivered to the recipient actors as identified in Table 1-5.

1.5.2 Phase 2: Manufacturing

Step 3: Manufacture of the IC

The **IC Manufacturer** produces the TOE integrated circuit, containing the IC Dedicated Software and the Embedded Software, and creates in the IC persistent memory the high-level objects relevant for the ICAO application.
Particularly, the initialization key is stored into the IC persistent memory.

Finally, the TOE is securely delivered to the **Card Manufacturer**.

Application Note 2 *The point of delivery of the TOE coincides with the completion of step 3, i.e. with the delivery of the TOE, in the form of an IC not yet embedded, from the IC Manufacturer to the Card Manufacturer. That is to say, this is the event upon which the construction of the TOE in a secure environment ends, and the TOE begins to be self-protected.*

Step 4: Manufacture of the smart card or document booklet

The **Card Manufacturer** equips the IC with contact-based and/or contactless interfaces, and embeds the IC into a smart card or a document booklet.

Finally, the TOE is securely delivered to the **Initialization Agent**.

Step 5: Initialization

The **Initialization Agent** sends the encrypted product information and/or configuration data (if any), as well as the encrypted pre-personalization key, to the TOE, which deciphers the cryptograms using the initialization key, verifies the correctness of the resulting plaintexts, and stores the data into persistent memory.

Finally, the TOE is securely delivered to the **Pre-personalization Agent**, along with the pre-personalization key if it was delivered to the **Initialization Agent** rather than directly to the **Pre-personalization Agent**.

As regards TOE guidance documentation, if the **Initialization Agent** also received the documents intended for the subsequent actors, then either all of these documents are securely delivered to the **Pre-personalization Agent**, or each document is securely delivered to the recipient actors as identified in Table 1-5.

Step 6: Pre-personalization

The **Pre-personalization Agent** generates the personalization key, then creates/modifies in the IC persistent memory the high-level objects relevant for the ICAO application.

Once the pre-personalization is finished, the TOE and the personalization key are securely delivered to the **Personalization Agent**.

As regards TOE guidance documentation, if the **Pre-personalization Agent** also received the documents intended for the subsequent actors, then either all of these documents are securely delivered to the **Personalization Agent**, or each document is securely delivered to the recipient actors as identified in Table 1-5.

1.5.3 Phase 3: Personalization

Step 7: Personalization

The personalization of the e-Document, performed by the **Personalization Agent**, includes:

(i) the survey of the e-Document holder's biographical data,

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

(iii) the personalization of the visual readable data onto the physical part of the e-Document,

(iv) the writing of the TOE user data and TSF data into the logical e-Document, and

(v) configuration of the TSF if necessary.

Step (iv) 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 [R22] [R24] finalizes the personalization of the genuine e-Document for the document holder.

Application Note 3 *The authenticated Personalization Agent shall additionally verify an Application Secret Code (ASC) to have read access to user data stored in step 6.*

The personalized e-Document (together with appropriate guidance for TOE use if necessary) is handed over to the **e-Document holder** for operational use.

Application Note 4 *The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [R16], section 92) comprise (but are not limited to) the initialization key, the pre-personalization key, the personalization key, and the Basic Access Control key.*

Application Note 5 *This security target distinguishes between the Personalization Agent as an entity known to the TOE and the Document Signer as an entity in the TOE IT environment signing the Document Security Object as described in [R22] and [R24]. This approach allows but does not enforce the separation of these roles.*

1.5.4 Phase 4: Operational use

Step 8: Inspection

The TOE is used as e-Document's chip by the presenter and the inspection systems in the operational use phase. The user data can be read and used according to the security policy of the issuing state or organization, but can never be modified.

Application Note 6 *This ST considers phase 1 and parts of phase 2 (i.e. step 1 to step 3) as part of the evaluation, and therefore defines the TOE delivery according to CC after*

step 3. Since specific production steps of phase 2 are of minor security relevance (e.g. card manufacturing and antenna integration), these are not part of the CC evaluation under ALC. Note that the personalization process and its environment may depend on specific security needs of an issuing state or organization. All production, generation, and installation procedures, after TOE delivery up to the operational use (phase 4), have to be considered in the product evaluation process under AGD assurance class. Therefore, this security target outlines the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.
Some production steps, e.g. step 6 in phase 2, may also take place in phase 3.

1.6 TOE description

1.6.1 Physical scope of the TOE

The TOE is comprised of the following parts:

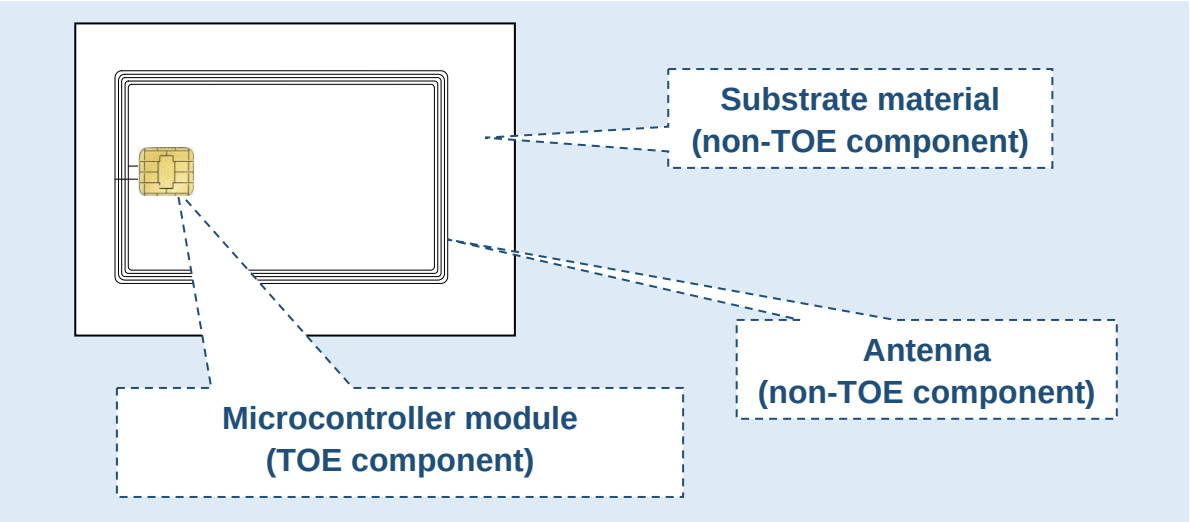
- dual-interface chip Samsung S3D350A (rev2) equipped with IC Dedicated Software (cf. Appendix A for more details);
- smart card operating system SOMA-c018;
- an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303 [R22] [R23] [R24];
- guidance documentation about the initialization of the TOE and the preparation and use of the ICAO application, composed by:
    - the Initialization Guidance [R4],
    - the Pre-personalization Guidance [R5],
    - the Personalization Guidance [R6],
    - the Operational User Guidance [R7].

Table 1-5 identifies, for each guidance document, the actors involved in TOE life cycle who are the intended recipients of that document.
The TOE is distributed in accordance with the evaluated delivery procedure [R8].

1.6.2 Other non-TOE physical components

The antenna and the substrate are not part of the TOE.
Figure 1-2 shows the physical components, distinguishing between TOE components and non-TOE components.

Figure 1-2 Smart card physical components



1.6.3 Logical scope of the TOE

The SOMA-c018 operating system manages all the resources of the integrated circuit that equips the e-Document, providing secure access to data and functions.
In more detail, in each life cycle phase/step, access to data and functions is restricted by means of cryptographic mechanisms as follows:

- In step 5, Initialization, of phase 2, the Initialization Agent must prove his/her identity by means of an authentication mechanism based on AES with 256-bit key.
- In step 6, Pre-personalization, of phase 2, the Pre-personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In phase 4, Operational use, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2, and DG5 to DG16, by means of the PACE mechanism compliant to ICAO Doc 9303-11 [R23]. Access to sensitive data, i.e. DG3 and DG4, is allowed after the genuineness of the IC has been proven by means of the Chip Authentication mechanism defined in [R23], and after the user has proven his/her entitlement by means of the Terminal Authentication mechanism as defined in [R13].

After a successful authentication, the communication between the e-Document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification [R29].

The integrity of the data stored under the LDS can be checked by means of the Passive

Authentication mechanism defined in [R23]. The Active Authentication mechanism defined in [R23] may be used as an alternative technique to ascertain the genuineness of the chip. However, access to sensitive data requires the use of the Chip Authentication mechanism. Passive Authentication, PACE, Active Authentication, Chip Authentication, and EAC mechanisms are described in more detail in the following subsections.

1.6.3.1 Passive Authentication

Passive Authentication consists of the following steps (cf. [R23]):

1. The inspection system reads the Document Security Object (SO_D), which contains the Document Signer Certificate (C_{DS}, cf. [R22]), 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 (SO_D) according to [R24].

3. The inspection system uses the verified Document Signer Public Key (KPu_{DS}) to verify the signature of the Document Security Object (SO_D).

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 (SO_D).

1.6.3.2 Password Authenticated Connection Establishment

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

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

- Strong session keys are provided independently of the strength of the password.

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

PACE supports, as part of the protocol execution, different mappings of the generator of the cryptographic group contained in the selected domain parameters into an ephemeral one. The following mappings are supported by the TOE:

- *Generic Mapping*, based on a Diffie-Hellman key agreement;
- *Chip Authentication Mapping*, which extends Generic Mapping and integrates Chip Authentication into the PACE protocol.

1.6.3.3 Active Authentication

Active Authentication authenticates the IC by signing a challenge sent by the inspection system with a private key known only to the IC (cf. [R23]).

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

By authenticating the Document Security Object (SO_D) and Data Group 15 by means of Passive Authentication (cf. section 1.6.3.1) in combination with Active Authentication, the inspection system verifies that the Document Security Object (SO_D) has been read from a genuine IC.

In accordance with ICAO Doc 9303 [R23], the ICAO application supports plain signature format according to [R15]. Only prime curves with uncompressed points shall be used. A hash algorithm, whose output length is of the same length or shorter than the length of the ECDSA key in use, shall be used, with hash algorithm SHA-256 compliant with FIPS PUB 180-4 [R36] and keys at least of 256 bits to a maximum of 512 bits.

1.6.3.4 Chip Authentication

Chip Authentication is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the e-Document chip (cf. [R23]).

The main differences with respect to Active Authentication are:

- Challenge Semantics is prevented because the transcripts produced by this protocol are non-transferable.

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

Details on Challenge Semantics are described in [R23].

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

- The private key is stored securely in the e-Document chip's memory.

- The public key is stored in Data Group 14.

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

In accordance with ICAO Doc 9303 [R23], the ICAO application supports Diffie-Hellman key agreement for Chip Authentication on elliptic curve groups over prime fields (ECDH algorithm, cf. [R15]), with keys of 224, 256, 320, 384, 512 bits.

Chip Authentication may be performed either as a distinct protocol, or as part of the PACE protocol in case Chip Authentication Mapping is used.

1.6.3.5 Extended Access Control

According to [R23], Extended Access Control is a security mechanism by means of which the e-Document chip authenticates the inspection systems authorized to read the optional biometric reference data and protects access to these data.

Following BSI TR-03110 [R13] [R14], the ICAO application enforces Extended Access Control through the support of Terminal Authentication v1, which is a challenge-response protocol that provides explicit unilateral authentication of the terminal.

This protocol enables the e-Document chip to verify that the terminal is entitled to access sensitive data. Terminal Authentication also authenticates the ephemeral public key chosen by the terminal to set up secure messaging through Chip Authentication (cf. section 1.6.3.4) or PACE with Chip Authentication Mapping (cf. section 1.6.3.2). In this way, the e-Document chip binds the terminal's access rights to the secure messaging session established by the authenticated ephemeral public key of the terminal.

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

Following BSI TR-03110 [R13] [R14], the ICAO application supports Terminal Authentication with signature verification algorithm ECDSA (cf. [R15]). Hash algorithm SHA-256 (cf. [R36]) and keys of 224 or 256 bits are supported.

2. Conformance claims

2.1 Common Criteria conformance claim

This security target claims conformance to:

- Common Criteria version 3.1 revision 5 [R16] [R17] [R18], as follows:
  - Part 2 (security functional requirements) extended,
  - Part 3 (security assurance requirements) conformant.

The software part of the TOE runs on the chip Samsung S3D350A (rev2) (see Appendix A). This integrated circuit is certified against Common Criteria at the assurance level EAL6+ (cf. Appendix A).

2.2 Package conformance claim

This security target claims conformance to:

- EAL5 assurance package augmented by ALC_DVS.2 and AVA_VAN.5, as defined in CC part 3 [R18].

2.3 Protection Profile conformance claim

This security target claims strict conformance to:

- BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, December 2012 [R11],
- BSI-CC-PP-0068-V2-2011-MA-01, Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, July 2014 [R12].

2.4 Protection Profile conformance rationale

This ST claims strict conformance to the PACE PP [R12] and EAC PP [R11]. The parts of the TOE listed in those Protection Profiles correspond to the ones listed in section 1.4.1 of this ST.

This ST adopts as a reference the ICAO Doc 9303 Seventh Edition 2015. This new version includes the specification of the PACE protocol, and no longer uses the terms “Supplemental Access Control” and “SAC”. Due to this update, in this ST:

- any references to the ICAO Doc 9303 2006 specification in the EAC PP and in the PACE PP have been replaced with references to Doc 9303 2015,
- any references to the ICAO “Supplemental Access Control” specification have been replaced with references to Doc 9303 2015,
- the terms “Supplemental Access Control” and “SAC” in the PACE PP have been replaced with the terms “Password Authenticated Connection Establishment” and “PACE”.

Being the TOE a general purpose electronic document, all references in the PPs to the use of the TOE as a travel document have been removed in this ST. For the same reason, with respect to the PPs, in this ST the acronym “MRTD” has been replaced by the term “e-Document”, the term "travel document" has been replaced by the terms "e-Document" or "electronic document", and the term "traveller" has been replaced by the terms "user" or "presenter". Such changed terms are printed in blue.

With respect to the PPs, the role “MRTD Manufacturer” has been split into the roles Card Manufacturer, Initialization Agent, and Pre-personalization Agent, acting in Phase 2 “Manufacturing” respectively in Step 4, Card Manufacturing, Step 5, Initialization, and Step 6, Pre-personalization. Note that the Card Manufacturer is a role performing only the physical preparation of the TOE.

In some parts of this ST the roles acting in Phase 2, i.e. the IC Manufacturer, the Card Manufacturer, the Initialization Agent, and the Pre-personalization Agent are collectively referred to as the Manufacturer.

In this ST, the TOE will be delivered from the IC Manufacturer to the Card Manufacturer after Step 3 “IC Manufacturing” of Phase 2, as a chip, in accordance with Application Note 4 of the EAC PP [R11]. At TOE delivery, there is no user data or machine readable data available. The EF.DG14 and EF.DG15 files, containing part of the user data, are written by the Pre-personalization Agent in Step 6 “Pre-Personalization” of Phase 2. The remaining user data as well as applicative files are written by the Personalization Agent, during Phase 3 “Personalization”.

Concerning Initialization Data, this ST distinguishes between IC Initialization Data written in Step 3 by the IC Manufacturer and TOE Initialization Data written in Step 5 by the Initialization Agent.

Concerning Initialization Data, this ST distinguishes between IC Initialization Data written in Step 3 by the IC Manufacturer and TOE Initialization Data written in Step 5 by the Initialization Agent.

The TOE provides a contact interface according to ISO/IEC 7816-2 [R28]; therefore, in addition to the contactless interface referred in the PPs, this ST makes also references to the contact interface.

This ST adds some notes to warn about usage of the algorithm Triple-DES, which is legacy, and of the hash function SHA-1, which is deprecated. However, for PACE, Chip Authentication and Terminal Authentication these algorithms are required and therefore they are included in the scope of the evaluation. The use of these algorithms is not deprecated for PACE, Chip Authentication and Terminal Authentication.

The security problem definition includes the assets, the subjects, the assumptions, the threats, and the organizational security policies of both PPs. Table 2-1 specifies the source (PACE PP or EAC PP) of assumptions, threats, and organizational security policies.

Table 2-1 Source of assumptions, threats, and OSPs

	Source	
	PACE PP [R12]	**EAC PP [R11]**
Assumptions	• A.Passive_Auth	• A.Insp_Sys • A.Auth_PKI
Threats	• T.Skimming • T.Eavesdropping • T.Tracing • T.Forgery • T.Abuse-Func • T.Information_Leakage • T.Phys-Tamper • T.Malfunction	• T.Read_Sensitive_Data • T.Counterfeit
Organizational Security Policies	• P.Manufact • P.Pre-Operational • P.Card_PKI • P.Trustworthy_PKI • P.Terminal	• P.Sensitive_Data • P.Personalization

The security objectives of both PPs are included in this ST. Table 2-2 specifies the source (PACE PP or EAC PP) of security objectives for the TOE and of security objectives for the operational environment.

Table 2-2 Source of security objectives

	Source	
	PACE PP [R12]	**EAC PP [R11]**
Security objectives for the TOE	• OT.Data_Integrity • OT.Data_Authenticity • OT.Data_Confidentiality • OT.Tracing • OT.Prot_Abuse-Func • OT.Prot_Inf_Leak • OT.Prot_Phys-Tamper • OT.Prot_Malfunction • OT.Identification • OT.AC_Pers	• OT.Sens_Data_Conf • OT.Chip_Aut_Proof
Security objectives for the operational environment	• OE.Personalization • OE-Passive_Auth_Sign • OE.Terminal • OE.e-Document_Holder • OE.Legislative_Compliance	• OE.Chip_Auth_Key_e-Document • OE.Authoriz_Sens_Data • OE.Exam_e-Document • OE.Prot_Logical_e-Document • OE.Ext_Insp_Systems

Note that the objective named OE.Auth_Key_Travel_Document in the EAC PP has been renamed to OE.Chip_Auth_Key_e-Document to distinguish it from the similar objective that has been added to this ST to cover the Active Authentication (see Table 2-3 below).

Table 2-3 describes the changes and additions made to the security problem definition and to the security objectives with respect to the PPs [R11] [R12].

Table 2-3 Modified elements in the security problem definition and security objectives

Element	Definition	Operation
A.Insp_Sys	Inspection Systems for global interoperability	The definition has been extended to take into account the fact that if PACE-CAM is performed, there is no need to perform Chip Authentication v1.

Element	Definition	Operation
P.Manufact	Manufacturing of the e-Document's chip	Modified to specify the storage of e-Document's Manufacturer keys, DG14, and DG15.
P.Pre-operational	Pre-operational handling of the e-Document	Modified to add the Initialization Agent and the Pre-personalization Agent among the subjects authorized by the e-Document issuer.
OT.AC_Init	Access control for Initialization of e-Document	Added to take into account access control in Step 5, Initialization.
OT.AC_Pre-pers	Access control for Pre-personalization of e-Document	Added to take into account access control in Step 6, Pre-personalization.
OT.AC_Pers	Access control for Personalization of e-Document	For consistency with OT.AC_Pre-pers, the definition now precisely indicates which data are written in Personalization.
OT.Active_Auth_Proof	Proof of e-Document's chip authenticity by Active Authentication	Added to cover the proof of IC authenticity for Basic Inspection Systems.
OT.Chip_Auth_Proof	Proof of the e-Document's chip authenticity	The definition from PP56 [R11] has been extended to take into account the fact that chip authenticity may also be proved by means of PACE-CAM.
OT.Identification	Identification of the TOE	Modified to specify that the Initialization Data are split into IC Initialization Data and TOE Initialization Data, that IC Initialization Data include the Initialization Key, and that TOE Initialization Data include the Pre-personalization Keys.
OT.Tracing	Tracing e-Document	The definition from PP68 has been extended to take into account the presence of a contact interface.
OE.Active_Auth_Key_e-Document	e-Document Active Authentication key	Added to cover the generation, signature and storage of the Active Authentication key pair, as well as the support to the Inspection System.
OE.Exam_e-Document	Examination of the physical part of the e-Document	The definition from PP56 [R11] has been extended to take into account the fact that chip authenticity may also be proved by means of PACE-CAM.
OE.Initialization	Initialization of e-Document	Added to take into account responsibilities in Step 5, Initialization.

Element	Definition	Operation
OE.Pre-personalization	Pre-personalization of e-Document	Added to take into account responsibilities in Step 6, Pre-personalization.

The security functional requirements described in section 6 of this ST include the SFRs of both the PACE PP [R12] and the EAC PP [R11].
Table 2-4 specifies the source (PACE PP or EAC PP) of security functional requirements.

Table 2-4 Source of security functional requirements

	Source	
	PACE PP [R12]	**EAC PP [R11]**
Security functional requirements	• FCS_CKM.1/DH_PACE • FCS_CKM.4 • FCS_COP.1/PACE_ENC • FCS_COP.1/PACE_MAC • FCS_RND.1 • FIA_AFL.1/PACE • FIA_UID.1/PACE • FIA_UAU.1/PACE • FIA_UAU.4/PACE • FIA_UAU.5/PACE • FIA_UAU.6/PACE • FDP_ACC.1/TRM • FDP_ACF.1/TRM • FDP_RIP.1 • FDP_UCT.1/TRM • FDP_UIT.1/TRM • FTP_ITC.1/PACE • FAU_SAS.1 • FMT_SMF.1 • FMT_SMR.1/PACE • FMT_LIM.1 • FMT_LIM.2 • FMT_MTD.1/INI_ENA • FMT_MTD.1/INI_DIS • FMT_MTD.1/KEY_READ	• FCS_CKM.1/CA • FCS_COP.1/CA_ENC • FCS_COP.1/SIG_VER • FCS_COP.1/CA_MAC • FIA_API.1 • **FIA_UID.1/PACE** • **FIA_UAU.1/PACE** • **FIA_UAU.4/PACE** • **FIA_UAU.5/PACE** • FIA_UAU.6/EAC • **FDP_ACC.1/TRM** • **FDP_ACF.1/TRM** • **FMT_SMR.1/PACE** • **FMT_LIM.1** • **FMT_LIM.2** • FMT_MTD.1/CVCA_INI • FMT_MTD.1/CVCA_UPD • FMT_MTD.1/DATE • FMT_MTD.1/CAPK • **FMT_MTD.1/KEY_READ** • FMT_MTD.3 • **FPT_EMS.1**

	• FMT_MTD.1/PA • FPT_EMS.1 • FPT_FLS.1 • FPT_TST.1 • FPT_PHP.3	

In the above table, note the following points:

- The EAC PP SFRs written in bold text cover the definition in PACE PP and extend them for EAC. These extensions do not conflict with strict conformance to PACE PP.
- An iteration label has been added to the EAC PP SFRs printed in underlined text, to distinguish them from the similar SFRs that have been added to this ST (see Table 2-5 below). The requirement definitions remain unchanged with respect to the PP.

Iterations and changes to the SFRs, with respect to PACE PP and EAC PP, are listed in Table 2-5. These changes do not lower TOE security.

Table 2-5 Additions, iterations, and changes to SFRs

Security functional requirement	Operation
FCS_CKM.1/CPS	**Iteration** This iteration has been added to cover the generation of the session keys for the Pre-personalization Agent and for the Personalization Agent.
FCS_CKM.1/GIM	**Iteration** This iteration has been added to cover the generation of the Initialization Key.
FCS_CKM.1/DH_PACE	**Change in dependency rationale** It has been found that some components fulfil dependency from FCS_COP.1. Therefore Justification 4 has been removed.
FIA_API.1/AA	**Iteration** This iteration has been added to cover the proof of identity by means of Active Authentication.

Security functional requirement	Operation
FIA_API.1/CAV1 FIA_API.1/CAM	**Iteration** An iteration labelled 'CAM' has been added to take into account PACE-CAM as an additional mechanism that the TOE must provide. The iteration label 'CAV1' has been added to better distinguish it from the other iteration.
FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers	**Iteration** Iterations have been added to distinguish between authentication failure handling throughout pre-operational TOE life cycle
FIA_AFL.1/Init	**Refinement** This SFR has been refined with respect to the PP to indicate that the initialization key is blocked after 31 authentication attempts, regardless of the outcome of the authentication. This refinement makes the SFR more restrictive.
FCS_COP.1/AUTH	**Iteration** This iteration has been added to cover the cryptographic mechanisms used in the authentication of the Initialization Agent, the Pre-personalization Agent and the Personalization Agent.
FCS_COP.1/AA_SIGN	**Iteration** This iteration has been added to cover the signature of Active Authentication data.
FMT_MTD.1/AAPK	**Iteration** This iteration has been added to restrict the ability to cover the writing of the Active Authentication private key.
FIA_UAU.4/PACE	**Change of Application Note** The application note now clarifies that this SFR also relates to the authentication of the Initialization Agent and the Pre-personalization Agent (cf. Application Note 68).
FIA_UAU.5.2/PACE	**Refinement** The specification concerning Terminal Authentication takes into account the fact that session keys established during PACE-CAM may also be used. An alternative condition has been added for the TOE to accept authentication attempts by means of Terminal Authentication.
FIA_UAU.6/EAC/CAV1 FIA_UAU.6/EAC/CAM	**Iteration** An iteration labelled 'EAC/CAM' has been added to take into account PACE-CAM as an additional condition. The iteration label 'CAV1' has been added to the original SFR from the PP to distinguish it from the other iteration.
FPT_EMS.1.2	**Refinement** A refinement has been added to better specify access to data through contact interface.

Security functional requirement	Operation
FTP_ITC.1/CPS	**Iteration** This iteration has been added to require data to be exchanged through a secure channel in Pre-personalization and in Personalization.
FCS_CKM.1/CA FCS_COP.1/SIG_VER FIA_UAU.6/EAC	**Change in SFRs Rationale** With respect to EAC PP [R11], the SFRs listed on the right are not mapped to the objective OT.AC_Pers since neither Chip Authentication nor Terminal Authentication are used for authentication of the Personalization Agent.

3. Security problem definition

Application Note 7 *With respect to the security problem definition contained in the PPs, this ST has some additions concerning Active Authentication.*

3.1 Introduction

3.1.1 Assets

Due to strict conformance to both EAC PP [R11] and PACE PP [R12], this ST includes, as assets to be protected, all assets listed in section 3.1 of those PPs.

3.1.1.1 Assets to be protected according to PACE PP

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 section 10.2 for the term definitions).

Table 3-1 Primary assets

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
e-Document			
1	User data stored on the TOE	All data (being not authentication data) stored in the context of the ICAO application of the e-Document as defined in [R23] and being allowed to read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R23]). This asset covers “User Data on the MRTD’s chip”, “Logical MRTD Data” and “sensitive User Data” in [R10].	Confidentiality[4] Integrity Authenticity
2	User data transferred between	All data (being not authentication data) being transferred in the context of the ICAO	Confidentiality[5] Integrity

[4] Though not each data element stored on the TOE represents a secret, the specification [R23] anyway requires securing their confidentiality: only terminals authenticated according to [R23] can get access to the user data stored. They have to be operated according to P.Terminal.

[5] Though not each data element being transferred represents a secret, the specification [R23] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [R23].

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
	the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	application of the e-Document as defined in [R23] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R23]). User data can be received and sent (exchange ⇔ {receive, send}).	Authenticity
3	e-Document tracing data	Technical information about the current and previous locations of the e-Document gathered unnoticeable by the e-Document holder recognising the TOE not knowing any PACE password. TOE tracing data can be provided/gathered.	Unavailability[6]

Application Note 8 *Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the e-Document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current PP also secures these specific e-Document holder's data as stated in the table above.*

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

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are listed in Table 3-2.

Table 3-2 Secondary assets

Object No.	Asset	Definition	Property to be maintained by the current security policy
e-Document			
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.	Availability

[6] Represents a prerequisite for anonymity of the e-Document holder.

Object No.	Asset	Definition	Property to be maintained by the current security policy
		This asset also covers “Authenticity of the MRTD’s chip” in [R10].	
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SO_D containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	e-Document communication establishment authorization data	Restricted-revealable[7] authorization information for a human user being used for verification of the authorization attempts as authorised user (PACE password). These data are stored in the TOE and are not to be sent to it.	Confidentiality Integrity

Application Note 9 *Since the e-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 e-Document holder is using TOE.*

Application Note 10 *e-Document communication establishment authorization data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorization attempt.*
The TOE shall secure the reference information as well as – together with the terminal connected[8] - 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.

3.1.1.2 Assets to be protected according to EAC PP

Logical e-Document sensitive User Data

[7] The e-Document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.
[8] The e-Document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.

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

Application Note 11 *Due to interoperability reasons, the ICAO Doc 9303-11 [R23] requires that Basic Inspection Systems may have access to logical e-Document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode according to this ST, if it is accessed using BAC [R23] (conformance to the BAC certification [R3] is kept, though). Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [R10]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform either PACE-CAM or Chip Authentication v.1 before getting access to data (except DG14), as these mechanisms are resistant to potential attacks.*

A sensitive asset is the following more general one.

Authenticity of the e-Document's chip

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

3.1.2 Subjects

This security target considers the subjects defined in the PACE PP and in the EAC PP. The subjects considered in accordance with the PACE PP 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	e-Document holder	A person for whom the e-Document Issuer has personalised the e-Document[9]. This entity is commensurate with e-Document Holder in [R10]. Please note that an e-Document holder can also be an attacker (see below external entity No.9).
2	-	e-Document presenter	A person presenting the e-Document to a terminal[10] and claiming the identity of the e-Document holder. This external entity is commensurate with "Traveller" in [R10].

[9] That is, this person is uniquely associated with a concrete e-Document

[10] In the sense of [R23]

External Entity No.	Subject No.	Role	Definition
			Please note that an e-Document presenter can also be an attacker (see below external entity No.9).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contact or contactless interfaces. 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 e-Document presenter). This entity is commensurate with "Terminal" in [R10].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspection authority[11] and verifying the e-Document presenter as the e-Document holder (for e-Document: by comparing the real biometric data (face) of the e-Document presenter with the stored biometric data (DG2) of the e-Document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the e-Document using a shared password (PACE password) and supports Passive Authentication.
5	-	Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the e-Document for passive authentication. A Document Signer is authorised by the CSCA issuing the Document Signer Certificate (C_{DS}), see [R24]. This role is usually delegated to a Personalization Agent.
6	-	Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the e-Document Issuer with respect to confirming correctness of user and TSF data stored in the e-Document. The CSCA represents the country specific root of the PKI for the e-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 [R24].
7	4	Personalization Agent	An organization acting on behalf of the e-Document Issuer to personalise the e-Document for its holder by some or all of the following activities (i) establishing the identity of the e-Document holder, (ii) enrolling the biometric reference data of the e-Document holder, (iii) writing a subset of these data on the physical e-Document (optical personalization) and storing them in the e-Document (electronic personalization) for the e-Document holder as defined in [R23], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [R22] (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 e-Document Issuer.

[11] Concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			This entity is commensurate with “Personalization Agent” in [R22].
8	5	Manufacturer	Generic term collectively identifying the IC Manufacturer, the Card Manufacturer, the Initialization Agent, and the Pre-personalization Agent. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase. This entity is commensurate with “Manufacturer” in [R10].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, 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 to “Attacker” in [R10].

Application Note 12 *The subject “Basic Inspection System with BAC” (BIS-BAC) is described in another ST [R3].*

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

- **Country Verifying Certification Authority:** The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the e-Document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

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

- **Terminal**: A terminal is any technical system communicating with the TOE through the contact or contactless interfaces.

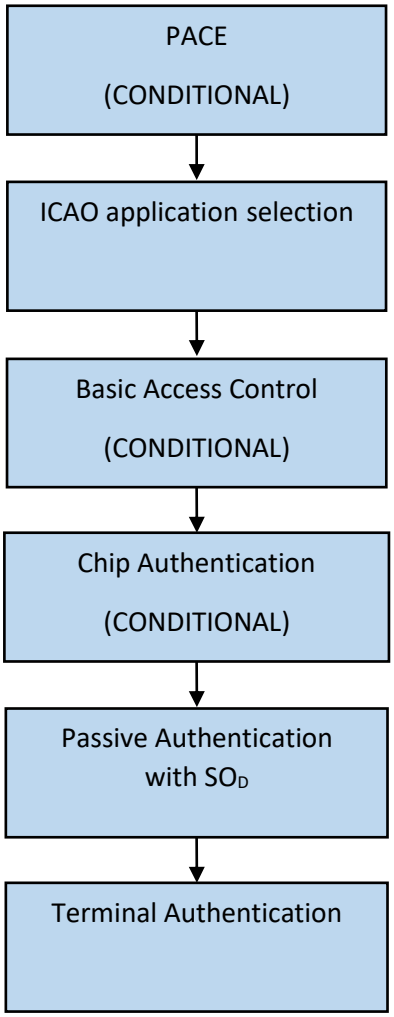
- **Inspection system (IS)**: A technical system used by the border control officer of the receiving State (i) in examining an e-Document presented by the user and verifying its authenticity and (ii) verifying the presenter as e-Document holder.

  The **Extended Inspection System (EIS)** performs the Advanced Inspection Procedure (see Figure 3-1) and therefore (i) contains a terminal for the contact or contactless communication with the e-Document's chip, (ii) implements the terminals part of PACE and/or BAC, (iii) gets the authorization to read the logical e-Document either under PACE or BAC by optical reading the e-Document providing this information, (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [R13], and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

- **Attacker**: In addition 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 e-Document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (ii) to forge a genuine e-Document, or (iv) to trace an e-Document.

Application Note 13 *An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged e-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 Advanced Inspection Procedure



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

3.2 Assumptions

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

3.2.1 A.Passive_Auth

PKI for Passive Authentication

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical e-Document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair.
The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity.
The Document Signer:

i. generates the Document Signer Key Pair,
ii. hands over the Document Signer Public Key to the CA for certification,
iii. keeps the Document Signer Private Key secret, and
iv. uses securely the Document Signer Private Key for signing the Document Security Objects of the e-Documents.

The CA creates the Document Signer Certificates for the Document Signer Public Keys and distributes them to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of the genuine user data according to [R22].

3.2.2 A.Insp_Sys

Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [R23] and/or BAC [R10]. 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 e-Document under PACE or BAC and performs the Chip Authentication to verify the logical e-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 Organization 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 [R12], as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

3.2.3 A.Auth_PKI

PKI for Inspection Systems

The issuing and receiving States or Organizations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organizations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their e-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 [R12] 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.

3.3 Threats

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

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

3.3.1 T.Skimming

Skimming e-Document/Capturing Card-Terminal Communication

Adverse action: An attacker imitates an inspection system in order to get access to the *user data stored on* or *transferred between the TOE and the inspecting authority connected* via the 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 e-Document data

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

Application Note 15 *The shared PACE password may be printed or displayed on the e-Document. Please note that if this is the case, the password does not effectively represent a secret, but nevertheless it is restricted-revealable, cf. OE.e-Document_Holder.*

3.3.2 T.Eavesdropping

Eavesdropping on the communication between the TOE and the PACE terminal

Adverse action: An attacker is listening to the communication between the e-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 e-Document data

Application Note 16 *A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.*

3.3.3 T.Tracing

Tracing e-Document

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

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

Asset: privacy of the e-Document holder

Application Note 17 *This threat completely covers and extends "T.Chip-ID" from BAC PP [R10].*

Application Note 18 *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.*

3.3.4 T.Forgery

Forgery of data

Adverse action: An attacker fraudulently alters the User Data or/and TSF-data stored on the e-Document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed e-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 e-Document

3.3.5 T.Abuse-Func

Abuse of Functionality

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

Threat agent: having high attack potential, being in possession of one or more e-Documents

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document

Application Note 19 *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.*

3.3.6 T.Information_Leakage

Information Leakage from e-Document

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

Application Note 20 *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) 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).*

3.3.7 T.Phys_Tamper

Physical Tampering

Adverse action: An attacker may perform physical probing of the e-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 e-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 e-Document.

Threat agent: having high attack potential, being in possession of one or more legitimate e-Documents

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document, confidentiality of User Data and TSF-data of the e-Document

Application Note 21 *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 e-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 e-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.

3.3.8 T.Malfunction

Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction the e-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 e-Document outside the normal operating conditions, exploiting errors in the e-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 e-Documents, having information about the functional operation

Asset: integrity and authenticity of the e-Document, availability of the functionality of the e-Document, confidentiality of User Data and TSF-data of the e-Document

Application Note 22 *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.*

3.3.9 T.Read_Sensitive_Data

Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the e-Document's chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming (cf. [R3]) in respect of the attack path (communication interface) and the

motivation (to get data stored on the e-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 e-Document's chip as private sensitive personal data whereas the MRZ data and the portrait are visual readable on the physical e-Document as well.

Threat agent: having high attack potential, knowing the PACE password, being in possession of a legitimate e-Document

Asset: confidentiality of sensitive logical e-Document (i.e. biometric reference) data

3.3.10 T.Counterfeit

Counterfeit of e-Document's chip

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

Threat agent: having high attack potential, being in possession of one or more legitimate e-Documents

Asset: authenticity of logical e-Document data

3.4 Organizational Security Policies

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.

3.4.1 P.Manufact

Manufacturing of the e-Document's chip

The IC Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the key for the authentication of the Initialization Agent.
The Initialization Agent configures the OS (TOE Initialization Data) and writes the key for the authentication of the Pre-personalization Agent.
The Pre-personalization Agent writes the Pre-Personalization Data which contains at least the Personalization key, the Chip Authentication public key (EF.DG14), and the Active Authentication public key (EF.DG.15).
The Initialization Agent and the Pre-personalization Agent are agents authorized by the Issuing State or Organization only.

3.4.2 P.Pre-Operational

Pre-operational handling of the e-Document

1. The e-Document Issuer issues the e-Document and approves it using the terminals complying with all applicable laws and regulations.

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

3. The e-Document Issuer uses only such TOE's technical components (IC) which enable traceability of the e-Documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. section 1.5 above.

4. If the e-Document Issuer authorizes an Initialization Agent, a Pre-personalization Agent or a Personalization Agent to personalize the e-Document for e-Document holders, the e-Document Issuer has to ensure that the Initialization Agent, the Pre-personalization Agent and the Personalization Agent act in accordance with the e-Document Issuer's policy.

3.4.3 P.Card_PKI

PKI for Passive Authentication (issuing branch)

Application Note 23 *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 e-Document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the e-Document. For this aim, he runs a Country Signing Certification Authority (CSCA). The e-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 e-Document Issuer by strictly secure means, see [R23]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the e-Document Issuer, see [R24].

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 e-Documents.

3.4.4 P.Trustworthy_PKI

Trustworthiness of PKI

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

3.4.5 P.Terminal

Abilities and trustworthiness of terminals

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

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by e-Document holders as defined in [R23] [R24].

2. They shall implement the terminal parts of the PACE protocol [R23], of the Passive Authentication [R23] and use them in this order[12]. 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 e-Document [R22] [R23]).

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 PP.

3.4.6 P.Sensitive_Data

Privacy of sensitive biometric reference data

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

3.4.7 P.Personalization

Personalization of the e-Document by issuing State or Organization only

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical e-Document with respect to the e-Document holder. The personalization of the e-

[12] This order is commensurate with [R23]

Document for the holder is performed by an agent authorized by the issuing State or Organization only.

4. Security objectives

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

4.1 Security objectives for the TOE

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

4.1.1 OT.AC_Init

Access Control for Initialization of logical e-Document

The TOE must ensure that the initialization data, which include at least the OS configuration data and the Pre-personalization Key, can be written in Step 5 Initialization by an authorized Initialization Agent only. The above data may be written only during and cannot be changed after initialization.

4.1.2 OT.AC_Pre-pers

Access Control for Pre-personalization of logical e-Document

The TOE must ensure that the logical e-Document data in EF.DG14 and EF.DG15 under the LDS, as well as other TSF data can be written in step 6, pre-personalization, by an authorized Pre-personalization Agent only. The logical e-Document pre-personalization data under the LDS, which includes at least the EF.DG14 and EF.DG15, may be written only during and cannot be changed after pre-personalization.

4.1.3 OT.Data_Integrity

Integrity of Data

The TOE must ensure integrity of the User Data and the TSF-data[13] 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.

4.1.4 OT.Data_Authenticity

Authenticity of Data

The TOE must ensure authenticity of the User Data and the TSF-data[14] stored on it by enabling verification of their authenticity at the terminal-side[15]. 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)[16].

4.1.5 OT.Data_Confidentiality

Confidentiality of Data

The TOE must ensure confidentiality of the User Data and the TSF-data[17] by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

4.1.6 OT.Tracing

Tracing e-Document

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the e-Document directly through establishing a communication via the contact interface, or remotely through establishing or listening to a communication via contactless interface of

[13] Where appropriate, see Table 3-2 above
[14] Where appropriate, see Table 3-2 above
[15] Verification of SO_D
[16] Secure messaging after PACE authentication, see also [R23]
[17] Where appropriate, see Table 3-2 above

the TOE, without knowledge of the correct values of shared passwords (PACE passwords) in advance.

4.1.7 OT.Prot_Abuse-Func

Protection against Abuse of Functionality

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

4.1.8 OT.Prot_Inf_Leak

Protection against Information Leakage

The TOE must provide protection against disclosure of confidential User Data and/or TSF-data stored and/or processed in the e-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 24 *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.*

4.1.9 OT.Prot_Phys-Tamper

Protection against Physical Tampering

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF-data, and the e-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 charges (using tools used in solid-state physics research and IC failure analysis),

- manipulation of the hardware and its security features, 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.

4.1.10 OT.Prot_Malfunction

Protection against Malfunctions

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

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

4.1.11 OT.Identification

Identification of the TOE

The TOE must provide means to store IC Initialization Data[18], TOE Initialization Data, and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the e-Document. The storage of the IC Initialization Data includes writing of the Initialization key. The storage of the TOE Initialization Data includes writing of the Pre-personalization key(s). The storage of the Pre-Personalization data includes writing of the Personalization key(s).

4.1.12 OT.AC_Pers

Access Control for Personalization of logical e-Document

The TOE must ensure that the logical e-Document data in EF.DG1 to EF.DG13 and EF.DG16, the Document security object according to LDS [R22] and the TSF data can be written by an authorized Personalization Agent only. The logical e-Document data in

[18] Amongst other, IC identification data

EF.DG1 to EF.DG13 and EF.DG16, and the TSF data may be written only during and cannot be changed after personalization of the document.

Application Note 25 *The OT.AC_Pers implies that the data of the LDS groups written during personalization for e-Document holder (at least EF.DG1 and EF.DG2) cannot be changed using write access after personalization.*

4.1.13 OT.Sens_Data_Conf

Confidentiality of sensitive biometric reference data

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

4.1.14 OT.Chip_Auth_Proof

Proof of e-Document's chip authenticity

The TOE must support the Inspection Systems to verify the identity and authenticity of the e-Document's chip as issued by the identified issuing State or Organization by means of either the PACE-CAM as defined in [R23] or the Chip Authentication Version 1 as defined in [R13]. The authenticity proof provided by e-Document's chip shall be protected against attacks with high attack potential.

Application Note 26 *The OT.Chip_Auth_Proof implies the e-Document's chip to have (i) a unique identity as given by the e-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 e-Document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the e-Document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [R22] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.*

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

4.1.15 OT.Active_Auth_Proof

Proof of e-Document's chip authenticity

The TOE must support the Basic Inspection Systems to verify the identity and authenticity of the e-Document's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [R23]. The authenticity proof provided by e-Document's chip shall be protected against attacks with high attack potential.

4.2 Security objectives for the operational environment

e-Document Issuer as the general responsible

The e-Document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment.

4.2.1 OE.Legislative_Compliance

Issuing of the e-Document

The e-Document Issuer must issue the e-Document and approve it using the terminals complying with all applicable laws and regulations.

e-Document Issuer and CSCA: e-Document's PKI (issuing) branch

The e-Document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 23 above).

4.2.2 OE.Passive_Auth_Sign

Authentication of e-Document by Signature

The e-Document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the e-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 e-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 [R22]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [R22]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on e-Document.

4.2.3 OE.Initialization

Initialization of e-Document

The issuing State or Organization must ensure that the Initialization Agent acting on behalf of the issuing State or Organization

i. create the OS configuration data and TSF data for the e-Document,

initialize the e-Document together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

4.2.4 OE.Pre-personalization

Pre-personalization of e-Document

The issuing State or Organization must ensure that the Pre-personalization Agent acting on behalf of the issuing State or Organization

i. create DG14, DG15 and TSF data for the e-Document,

ii. pre-personalize the e-Document together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

4.2.5 OE.Personalization

Personalization of e-Document

The e-Document Issuer must ensure that the Personalization Agent acting on his behalf (i) establish the correct identity of the e-Document holder and create the biographical data for

the e-Document, (ii) enrol the biometric reference data of the e-Document holder, (iii) write a subset of these data on the physical Document (optical personalization) and store them in the e-Document (electronic personalization) for the e-Document holder as defined in [R22][19], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [R23] (in the role of a DS).

Terminal operator: Terminal's receiving branch

4.2.6 OE.Terminal

Terminal operating

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by e-Document holders as defined in [R23].

2. The related terminals implement the terminal parts of the PACE protocol [R23], of the Passive Authentication [R23] (by verification of the signature of the Document Security Object) and use them in this order[20]. 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 e-Document (determination of the authenticity of data groups stored in the e-Document, [R23]).

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 27 *OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [R10].*

[19] See also [R23].

[20] This order is commensurate with [R23]

e-Document holder Obligations

4.2.7 OE.e-Document_Holder

e-Document holder Obligations

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

Issuing State or Organization

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

4.2.8 OE.Chip_Auth_Key_e-Document

e-Document Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the e-Document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the e-Document's chip used for genuine e-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 to counter the threat T.Counterfeit, as it specifies the pre-requisite for the Chip Authentication which is one of the features of the TOE described only in this Security Target.

4.2.9 OE.Authoriz_Sens_Data

Authorization for Use of Sensitive Biometric Reference Data

The issuing State or Organization has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of e-Document holders to authorized receiving States or Organizations. The Country Verifying Certification Authority

of the issuing State or Organization generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Read_Sensitive_Data, the Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the features of the TOE described only in this Security Target.

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.

4.2.10 OE.Active_Auth_Key_e-Document

e-Document Active Authentication key

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the e-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 e-Document's chip used for genuine e-Document by certification of the Active Authentication Public Key by means of the Document Security Object.

Receiving State or Organization

The Receiving State or Organization will implement the following security objectives of the TOE environment.

4.2.11 OE.Exam_e-Document

Examination of the physical part of the e-Document

The inspection system of the receiving State or Organization must examine the e-Document presented by the user to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the e-Document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [4] and/or the Basic Access Control [6]. 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 e-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_e-Document also repeats partly the requirements from above 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 features of a e-Document with Extended Access Control.

4.2.12 OE.Prot_Logical_e-Document

Protection of data from the logical e-Document

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical e-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.

4.2.13 OE.Ext_Insp_Systems

Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organizations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical e-Document. The Extended Inspection System authenticates themselves to the e-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 Organizational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

4.3 Security objective rationale

Table 4-1 provides an overview for security objectives coverage.

Table 4-1 Security objective rationale

	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	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.Chip_Auth_Key_e-Document	OE.Active_Auth_Key_e-Document	OE.Authoriz_Sens_Data	OE.Exam_e-Document	OE.Prot_Logical_e-Document	OE.Ext_Insp_Systems	OE.Initialization	OE.Pre-personalization	OE.Personalization	OE-Passive_Auth_Sign	OE.Terminal	OE.e-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	X	X	X	X		
P.Sensitive_Data	X																	X			X							
P.Personalization						X							X											X				
P.Manufact				X	X								X									X	X					
P.Pre-Operational				X	X	X							X									X	X	X				X
P.Terminal																			X							X		
P.Card_PKI																									X			
P.Trustworthy_PKI																									X			
A.Insp_Sys																			X	X								
A.Auth_PKI																		X			X							
A.Passive_Auth																			X						X			

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

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contact or contactless interfaces. 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.e-Document_Holder*** ensures that a PACE session can only be established either by the e-Document holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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

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

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_Init*** requires the TOE to limit the write access for the e-Document to the trustworthy Initialization Agent (cf. ***OE.Initialization***). The security objective ***OT.AC_Pre-pers*** requires the TOE to limit the write access for the e-Document to the trustworthy Pre-personalization Agent (cf. ***OE.Pre-personalization***). The security objective ***OT.AC_Pers*** requires the TOE to limit the write access for the e-Document to the trustworthy Personalization Agent (cf. ***OE.Personalization***). The TOE will protect the integrity and authenticity of the stored and exchanged User Data or/and TSF-data as aimed by the security objectives ***OT.Data_Integrity*** and ***OT.Data_Authenticity***, respectively. The objectives ***OT.Prot_Phys-Tamper*** and ***OT.Prot_Abuse-Func*** contribute to protecting integrity of the User Data or/and TSF-data stored on the TOE. A terminal operator operating his terminals according to ***OE.Terminal*** and performing the Passive Authentication using the Document Security Object as aimed by ***OE.Passive_Auth_Sign*** will be able to effectively verify integrity and authenticity of the data received from the TOE. Additionally, the examination of the presented e-Document book or card according to ***OE.Exam_e-Document*** "Examination of the physical part of the e-Document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the e-Document.

The threat **T.Abuse-Func** addresses attacks of misusing TOE's functionality to manipulate or to disclosure the stored User- or TSF-data as well as to disable or to bypass the soft-

coded security functionality. The security objective ***OT.Prot_Abuse-Func*** ensures that the usage of functions having not to be used in the operational phase is effectively prevented.

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

The threat **T.Counterfeit** "Counterfeit of e-Document chip data" addresses the attack of unauthorized copy or reproduction of the genuine e-Document's chip. This attack is thwarted by chip an identification and authenticity proof required by ***OT.Chip_Auth_Proof*** "Proof of e-Document's chip authentication" using an authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by ***OE.Chip_Auth_Key_e-Document*** "e-Document Authentication Key". According to ***OE.Exam_e-Document*** "Examination of the physical part of the e-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 e-Document's chip.

In addition, the threat **T.Counterfeit** "Counterfeit of e-Document chip data" is countered by chip an identification and authenticity proof required by ***OT.Active_Auth_Proof*** "Proof of e-Document's chip authentication" 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_e-Document*** "e-Document Authentication Key".

The OSP **P.Manufact** "Manufacturing of the e-Document's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data and the Personalization data as being fulfilled by ***OT.Identification***. ***OT.AC_Init***, ***OT.AC_Pre-pers***, ***OE.Initialization***, and ***OE.Pre-personalization*** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorization of e-Document Manufacturers'. Note:

- The IC Manufacturer equips the TOE with the Initialization Key according to ***OT.Identification***, Identification and Authentication of the TOE. The security objective ***OT.AC_Init*** limits the management of TSF data and the management of TSF to the Initialization Agent.
- The Initialization Agent equips the TOE with the Pre-personalization key(s) according to ***OT.Identification***, Identification and Authentication of the TOE. The security objective ***OT.AC_Pre-pers*** limits the management of TSF data and the management of TSF to the Pre-personalization Agent.

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_Init***, ***OT.AC_Pre-pers***, ***OT.AC_Pers***, ***OE.Initialization***, ***OE.Pre-personalization***, and ***OE.Personalization*** together enforce the OSP's properties 'correctness of the User- and the TSF-data stored' and 'authorization of Personalization Agent'; ***OE.Legislative_Compliance*** is affine to the OSP's property 'compliance with laws and regulations'.

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

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

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

The OSP **P.Personalization** "Personalization of the e-Document by issuing State or Organization only" addresses the (i) the enrolment of the logical e-Document by the Personalization Agent as described in the security objective for the TOE environment ***OE.Personalization*** "Personalization of logical e-Document", and (ii) the access control for the user data and TSF data as described by the security objective ***OT.AC_Pers*** "Access Control for Personalization of logical e-Document". Note:

- The Pre-personalization Agent equips the TOE with the Personalization key(s) according to ***OT.Identification*** "Identification and Authentication of the TOE". The security objective ***OT.AC_Pers*** limits the management of TSF data and the management of TSF to the Personalization Agent.

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

The OSP **P.Terminal** “Abilities and trustworthiness of terminals” is countered by the security objective ***OE.Exam_e-Document*** additionally to the security objectives from PACE PP [7]. ***OE.Exam_e-Document*** enforces the terminals to perform the terminal part of the PACE protocol.

The examination of the e-Document addressed by the assumption **A.Insp_Sys** “Inspection Systems for global interoperability” is covered by the security objective for the TOE environment ***OE.Exam_e-Document*** “Examination of the physical part of the e-Document” which requires the inspection system to examine physically the e-Document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented e-Document’s chip. The security objective for the TOE environment ***OE.Prot_Logical_e-Document*** “Protection of data from the logical e-Document” requires the Inspection System to protect the logical e-Document data during the transmission and the internal handling.

The assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment ***OE.Passive_Auth_Sign*** “Authentication of e-Document by Signature” from PACE PP [R12] 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_e-Document*** “Examination of the physical part of the e-Document”.

The assumption **A.Auth_PKI** “PKI for Inspection Systems” is covered by the security objective for the TOE environment ***OE.Authoriz_Sens_Data*** “Authorization for use of sensitive biometric reference data”, which requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organizations 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 Organization has to establish the necessary public key infrastructure.

5. Extended components definition

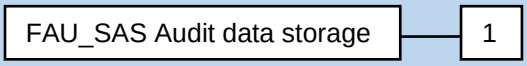
This security target uses components defined as extensions to CC part 2 [R17]. These components are drawn from the PACE PP [R12] and the EAC PP [R11].

5.1 Definition of family FAU_SAS

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

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

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 levelling:	
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 family FCS_RND

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional

requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

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 levelling:	FCS_RND Generation of random numbers — 1
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 family FIA_API

To describe the security requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [R11]. 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 28 *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 CC part 2 (cf. [R18] "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.*

Table 5-3 Family FIA_API

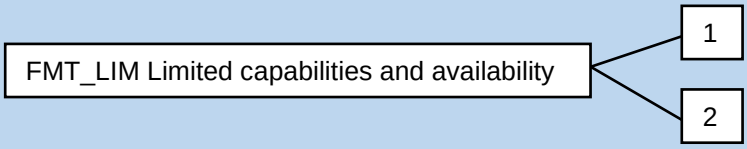
FIA_API Authentication Proof of Identity	
Family behaviour:	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
Component levelling:	FIA_API Authentication Proof of Identity — 1
FIA_API.1	Authentication Proof of 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 family FMT_LIM

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

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

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 levelling:	
FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
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 29 *The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that*

- *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

- *the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.*

The combination of both requirements shall enforce the related policy.

5.5 Definition of family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [R12].

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

Table 5-5 Family FPT_EMS

FPT_EMS	
Family behaviour:	This family defines requirements to mitigate intelligible emanations.
Component levelling:	FPT_EMS TOE emanation — 1
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 TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: specified limits] enabling access to [assignment: *list of types of TSF data*] and [assignment: list of types of user data].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6. Security functional requirements

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph C.4 of Part 1 [R16] of the CC. Each of these operations is used in this PP.

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.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text. Selections made by the ST author are denoted as **underlined bold text** and the original text of the component is given by a footnote.

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 as underlined text. Assignments made by the ST author are denoted as **underlined bold text** and the original text of the component is given by a footnote. In some cases, the assignment made by the PP authors defines a selection performed by the ST author. Thus, this text is underlined and italicized like *this*.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1.2. Note that all these subjects are acting for homonymous external entities. All used objects are defined either in section 10.2 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 [R17]. The operation "load" is synonymous to "import" used in [R17].
Table 6-1 provides the definition of security attributes.

Table 6-1 Definition of security attributes

Security attribute	Values	Meaning
Terminal authentication status	None (any terminal)	Default role (i.e. without authorization after start-up)
	CVCA	Role defined in the certificate used for authentication (cf. [R14]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	Role defined in the certificate used for authentication (cf. [R14]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	Role defined in the certificate used for authentication (cf. [R14]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	Role defined in the certificate used for authentication (cf. [R14]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal authorization	None	
	DG4 (iris)	Read access to DG4 (cf. [R14])
	DG3 (fingerprint)	Read access to DG3 (cf. [R14])
	DG3 (fingerprint)/DG4 (iris)	Read access to DG3 and DG4 (cf. [R14])

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

Table 6-2 Keys and certificates

Name	Data
Issuing PKI branch (from PACE PP [R12])	
Country Signing Certification Authority Key Pair and Certificate	The Country Signing Certification Authority of the e-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 [R24].
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 e-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}).
Session keys (from PACE PP [R12])	
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 Triple-DES Keys[21] for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE protocol, see [R23].
Ephemeral keys (from PACE PP [R12])	
PACE authentication ephemeral key pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE)	The ephemeral PACE Authentication Key Pair (ephem-SK_{PICC}-PACE, ephem-PK_{PICC}-PACE) is used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to BSI TR-03111 [R15], cf. [R23].
Receiving PKI branch (from EAC PP [R11])	
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying 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. [R14] and

[21] Usage ot the algorithm Triple-DES is deprecated.

Name	Data
	section 10.2). 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}) issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}) () the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Keys for chip authenticity verification (from EAC PP [R11])	
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Elliptic Curve Diffie-Hellman according to ISO 11770-3 [11].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical e-Document and used by the inspection system for Chip Authentication Version 1 of the e-Document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic e-Document's chip. It is part of the TSF data.
Chip Authentication Session Keys	Secure Messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
Active Authentication Key Pair	The Active Authentication Key Pair (SK_{AA}, PK_{AA}) is used for the Active Authentication mechanism in accordance with [R23].
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 genuineness of the e-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 e-Document's chip.
Other keys (from EAC PP [R11])	
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

Application Note 30 *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 the e-Document's point of view, the domestic Document Verifier belongs to the issuing State or Organization.*

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

6.1 Class FAU: Security audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

6.1.1 FAU_SAS.1

Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1:

The TSF shall provide the Manufacturer[22] with the capability to store the Initialization and Pre-personalization Data[23] in the audit records.

Application Note 31 *The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC Manufacturer, the Initialization Agent, and the Pre-personalization Agent in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF-Data into the TOE. The audit records are write-only-once data of the e-Document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).*

[22] [assignment: *authorised user*]

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

6.2 Class FCS: Cryptographic support

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

6.2.1 FCS_CKM.1/GIM

Cryptographic key generation – Generation of the Initialization Key by the TOE

Hierarchical to: No other components.

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

FCS_CKM.1.1/GIM:

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Initialization Key Generation Algorithm**[27] and specified cryptographic key sizes **256 bits**[28] that meet the following: **none**[29].

Application Note 32 *The TSF allows to generate the diversified 256-bit AES initialization key in Step 5, Initialization, of Phase 2, Manufacturing, by the algorithm described in the Initialization Guidance, using the key stored on the chip.*

6.2.2 FCS_CKM.1/CPS

Cryptographic key generation – Generation of CPS session Keys for Pre-personalization and Personalization by the TOE

Hierarchical to: No other components.

[24] [assignment: *cryptographic key generation algorithm*]
[25] [assignment: *cryptographic key sizes*
[26] [assignment: *list of standards*]
[27] [assignment: *cryptographic key generation algorithm*]
[28] [assignment: *cryptographic key sizes*
[29] [assignment: *list of standards*]

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

FCS_CKM.1.1/CPS:

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **CPS Keys Generation Algorithm**[30] and specified cryptographic key sizes **112 bits**[31] that meet the following: **[R20], section 5.2**[32].

Application Note 33 *The TSF allows to generate the session keys for the Pre-personalization and Personalization processes by the algorithm described in section 5.2 of the EMV CPS specification, [R20], using the keys stored on the chip (the Pre-personalization keys in phase 2 and the Personalization keys in phase 3) and a sequence counter provided by the IC card to the pre-personalization terminal or to the personalization terminal in response to an INITIALIZE UPDATE command.*

6.2.3 FCS_CKM.1/DH_PACE

Cryptographic key generation – Diffie-Hellman for PACE session keys

Hierarchical to: No other components.

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

FCS_CKM.1.1/DH_PACE:

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH compliant to [R15]**[33] and specified cryptographic key sizes: **224, 256, 320, 384, 512 bits**[34] that meet the following: [R23][35].

[30] [assignment: *cryptographic key generation algorithm*]
[31] [assignment: *cryptographic key sizes*
[32] [assignment: *list of standards*]
[33] [selection: *Diffie-Hellman protocol compliant to PKCS #3, ECDH compliant to BSI TR-03111*]
[34] [assignment: *cryptographic key sizes*]
[35] [assignment: *list of standards*]

Application Note 34 *The TOE generates a shared secret value K with the terminal during the PACE protocol, see [R23]. This protocol may be based on the ECDH compliant to TR-03111 [R15] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [R23] and [R15] 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 [R23] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.*

Application Note 35 *FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R23].*

Application Note 36 *Due to a restriction in the platform certification, as reported in the platform ST-lite [R1], only the following standard curves are admitted:*

- *NIST curves [R35]: P-224*, P-256, P-384;*
- *Brainpool curves [R27]: brainpoolP224r1*, brainpoolP224t1*, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1;*
- *SEC-recommended curves [R19]: secp224k1*, secp224r1*, secp256k1*, secp256r1*, secp384r1*.*

*Use of the curves marked with * is not recommended since they might not be secure enough for the actual state of the art.*

6.2.4 FCS_CKM.1/CA

Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA:

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ECDH**[36] and specified cryptographic key sizes **224, 256, 320, 384, 512 bits**[37]

[36] [assignment: *cryptographic key generation algorithm*]
[37] [assignment: *cryptographic key sizes*]

that meet the following: **based on an ECDH protocol compliant to [R15]**[38].

Application Note 37 *FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R13].*

Application Note 38 *The TOE generates a shared secret value with the terminal during the Chip Authentication protocol version 1, see [R13]. This protocol may be based on the ECDH compliant to TR-03111 [R15] (i.e. the elliptic curve cryptographic algorithm - cf. [R15] 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 [R13] [R14]).*

Application Note 39 *The TOE implements the hash functions SHA-1 and SHA-256 as cryptographic primitives to derive the keys for secure messaging from any shared secrets of the authentication mechanisms. However, usage of the hash function SHA-1 is deprecated outside PACE, Chip Authentication and Terminal Authenticate protocols.*

Application Note 40 *The TOE implements the hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [R13] [R14] for details).*

Application Note 41 *Chip Authentication session keys are not generated if PACE-CAM has been performed, as in this case Chip Authentication protocol version 1 is skipped.*

Application Note 42 *Due to a restriction in the platform certification, as reported in the platform ST-lite [R1], only the following standard curves are admitted:*

- *NIST curves [R35]: P-224*, P-256, P-384;*
- *Brainpool curves [R27]: brainpoolP224r1*, brainpoolP224t1*, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1;*
- *SEC-recommended curves [R19]: secp224k1*, secp224r1*, secp256k1*, secp256r1*, secp384r1*.*

*Use of the curves marked with * is not recommended since they might not be secure enough for the actual state of the art.*

[38] [selection: *based on the Diffie-Hellman key derivation protocol compliant to PKCS #3, based on an ECDH protocol compliant to BSI TR-03111*]

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

6.2.5 FCS_CKM.4

Cryptographic key destruction – Session keys

Hierarchical to: No other components.

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

FCS_CKM.4.1:

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **physical deletion by overwriting the memory data with zeros**[39] that meets the following: **none**[40].

Application Note 43 *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. (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. The TOE shall also destroy the Initialization Key.*

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

6.2.6 FCS_COP.1/AUTH

Cryptographic operation – Authentication

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

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

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH:

The TSF shall perform **symmetric authentication – encryption and decryption**[41] in accordance with a specified cryptographic algorithm **Triple-DES and AES**[42] and cryptographic key sizes: **112 bits for Triple-DES and 256 bits for AES**[43] that meet the following: **FIPS 46-3 [R34] and FIPS 197 [R38]**[44].

Application Note 44 *This SFR requires the TOE to implement the cryptographic primitive AES in CBC mode for authentication attempt of a terminal as Initialization Agent in Step 5 Initialization of Phase 2 Manufacturing, according to the mechanism described in the initialization guidance.*

Application Note 45 *This SFR requires the TOE to implement the cryptographic primitive Triple-DES for authentication attempt of a terminal as Pre-personalization Agent or as Personalization Agent by means of the CPS mechanism (cf. FIA_UAU.4).*

6.2.7 FCS_COP.1/AA_SIGN

Cryptographic operation – Signature for Active Authentication

Hierarchical to: No other components.

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

[41] [assignment: *list of cryptographic operations*]
[42] [selection: *Triple-DES, AES*]
[43] [selection: *112, 128, 168, 192, 256*]
[44] [selection: *FIPS 46-3, FIPS 197*]

FCS_COP.1.1/AA_SIGN:

The TSF shall perform **digital signature for Active Authentication data**[45] in accordance with a specific cryptographic algorithm **ECDSA with SHA-256**[46] and cryptographic key sizes **256, 320, 384 or 512 bits**[47] that meet the following: **Technical Guideline TR-03111 [R15] used for Active Authentication defined by ICAO Doc 9303-11 [R23]**[48].

Application Note 46 *This SFR has been added by the ST author to specify the cryptographic algorithm and key sizes used by the TOE to perform an Active Authentication in accordance with ICAO Doc 9303-11 [R23].*
It must be noted that according to section 6.1.2.3 of [R23], a hash algorithm, whose output length is of the same length or shorter than the length of the ECDSA key in use, shall be used.

Application Note 47 *Due to a restriction in the platform certification, as reported in the platform ST-lite [R1], only the following standard curves are admitted:*

- *NIST curves [R35]: curves P-256, P-384;*
- *Brainpool curves [R27]: brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1;*
- *SEC-recommended curves [R19]: secp256k1*, secp256r1*, secp384r1*.*

*Use of the curves marked with * is not recommended since they might not be secure enough for the actual state of the art.*

6.2.8 FCS_COP.1/PACE_ENC

Cryptographic operation – Encryption/Decryption AES/Triple-DES for PACE protocol

Hierarchical to: No other components.

[45] [assignment: *list of cryptographic operations*]
[46] [assignment: *cryptographic algorithm*]
[47] [assignment: *cryptographic key sizes*]
[48] [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]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/PACE_ENC:

The TSF shall perform secure messaging – encryption and decryption[49] in accordance with a specified cryptographic algorithm **AES and Triple-DES** in CBC mode[50] and cryptographic key sizes **112 bits (for Triple-DES) and 128, 192, 256 bits (for AES)**[51] that meet the following: compliant to [R23][52].

Application Note 48 *This SFR requires the TOE to implement the cryptographic primitive AES and Triple-DES for secure messaging with encryption of the transmitted data and encryption of 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 FCS_CKM.1/DH_PACE (PACE-K_{ENC}).*

Application Note 49 *Usage of the algorithm Triple-DES is deprecated.*

6.2.9 FCS_COP.1/PACE_MAC

Cryptographic operation – MAC for PACE protocol

Hierarchical to: No other components.

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

FCS_COP.1.1/PACE_MAC:

The TSF shall perform secure messaging – message authentication code[53] in accordance with a specified

[49] [assignment: *list of cryptographic operations*]
[50] [selection: *AES, Triple-DES*]
[51] [selection: 112, 128, 192, 256]
[52] [assignment: *list of standards*]
[53] [assignment: *list of cryptographic operations*]

cryptographic algorithm **CMAC and Retail MAC**[54] and cryptographic key sizes **112, 128, 192, 256 bits**[55] that meet the following: compliant to [R23][56].

Application Note 50 *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 [4] the (two-key) Triple-DES could be used in Retail mode for secure messaging. However, Retail mode is not recommended, as usage of the algorithm Triple-DES is deprecated.*

6.2.10 FCS_COP.1/CA_ENC

Cryptographic operation – Symmetric Encryption/Decryption for CA protocol

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[57] in accordance with a specified cryptographic algorithm **AES and Triple-DES**[58] and cryptographic key sizes **112 bits (for Triple-DES) and 128, 192, 256 bits (for AES)**[59] that meet the following: **ICAO Doc 9303-11 [R23]**[60].

Application Note 51 *This SFR requires the TOE to implement the cryptographic primitives (i.e. Triple-DES and AES) for secure messaging with encryption of the transmitted*

[54] [selection: *CMAC, Retail-MAC*]
[55] [selection: *112, 128, 192, 256*]
[56] [assignment: *list of standards*]
[57] [assignment: *list of cryptographic operations*]
[58] [assignment: *cryptographic algorithm*]
[59] [assignment: *cryptographic key sizes*]
[60] [assignment: *list of standards*]

data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication according to the FCS_CKM.1/CA.

Application Note 52 *Usage of the algorithm Triple-DES is deprecated.*

6.2.11 FCS_COP.1/CA_MAC

Cryptographic operation – MAC for CA protocol

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[61] in accordance with a specified cryptographic algorithm **CMAC and Retail MAC**[62] and cryptographic key sizes **112, 128, 192, 256 bits**[63] that meet the following: **ICAO Doc 9303-11 [R23]**[64].

Application Note 53 *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 by the TSF through Chip Authentication, performed either as part of PACE-CAM or by Chip Authentication Protocol Version 1 according to FCS_CKM.1/CA.*

6.2.12 FCS_COP.1/SIG_VER

Cryptographic operation – Signature verification by e-Document

Hierarchical to: No other components.

[61] [assignment: *list of cryptographic operations*]
[62] [assignment: *cryptographic algorithm*]
[63] [assignment: *cryptographic key sizes*]
[64] [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]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SIG_VER:

The TSF shall perform digital signature verification[65] in accordance with a specified cryptographic algorithm **ECDSA with SHA-256 as specified in Table 6-3**[66] and cryptographic key sizes: **224 or 256 bits**[67] that meet the following: **FIPS 186-4 [R37]**[68].

Table 6-3 ECDSA algorithms for signature verification in Terminal Authentication

Object identifier [R14]	Signature algorithm	Hash algorithm
id-TA-ECDSA-SHA-256	ECDSA	SHA-256

Application Note 54 *The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.*

Application Note 55 *For ECDSA cryptography, the TOE makes use of the Samsung cryptographic library.*

Application Note 56 *Due to a restriction in the platform certification, as reported in the platform ST-lite [R1], only the following standard curves are admitted:*

- *NIST curves [R35]: P-224*, P-256;*
- *Brainpool curves [R27]: brainpoolP224r1*, brainpoolP224t1*, brainpoolP256r1, brainpoolP256t*;*
- *SEC-recommended curves [R19]: secp224k1*, secp224r1*, secp256k1*, secp256r1*.*

*Use of the curves marked with * is not recommended since they might not be secure enough for the actual state of the art.*

[65] [assignment: *list of cryptographic operations*]
[66] [assignment: cryptographic algorithm]
[67] [assignment: *cryptographic key sizes*]
[68] [assignment: *list of standards*]

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

6.2.13 FCS_RND.1

Quality metrics 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 **BSI AIS-31 functionality class PTG.2 [R9] (see Application Note 58)**[69].

Application Note 57 *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.*

Application Note 58 *The TOE makes use of the digital true random number generator DTRNG FRO (library version 2.0) of the IC S3D350A (rev2). The DTRNG FRO (library version 2.0) has already been evaluated as conformant to class PTG.2 of BSI AIS31 [R9] with high strength of mechanism, provided that it is used as recommended in section 2.3.3 of [R43].*

6.3 Class FIA: Identification and authentication

For the sake of better readability, Table 6-4 provides an overview of the authentication mechanisms used.

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

Table 6-4 Overview of authentication SFRs

Mechanism	SFR for the TOE	Comments
Authentication Mechanism for Initialization Agent	FIA_AFL.1/Init FIA_UAU.4	AES (256-bit keys)
Authentication Mechanism for Pre-personalization Agent and Personalization Agent	FIA_UAU.4 FIA_AFL.1/Pre-pers FIA_AFL.1/Pers	Triple-DES (112-bit keys) Retail MAC (112-bit keys)
Chip Authentication Protocol v.1	FIA_API.1/CAV1 FIA_UAU.5 FIA_UAU.6	Triple-DES (112-bit keys) AES (128, 192, 256-bit keys) Retail MAC (112-bit keys) ECDH
Terminal Authentication Protocol v.1	FIA_UAU.5	ECDSA
PACE protocol[72]	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE FIA_API.1/CAM	ECDH with Generic Mapping and Chip Authentication Mapping
Passive Authentication	FIA_UAU.5/PACE	Verification of the hashes of DGs
Active Authentication	FIA_API.1/AA	ECDSA with SHA-256

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

The Chip Authentication may be performed as either part of PACE-CAM or as Chip Authentication protocol v.1. Both may be used independent of the Terminal Authentication Protocol v.1. If the Terminal Authentication Protocol v.1 is used, the terminal shall use the same public keys presented during either PACE-CAM or Chip Authentication Protocol v.1.

[70] Only listed for information purposes
[71] Only listed for information purposes
[72] Only listed for information purposes

6.3.1 FIA_AFL.1/Init

Authentication failure handling in Step 5 Initialization

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Init:

The TSF shall detect when **31**[77]
Refinement: authentication attempts
occur related to **authentication attempts (regardless of the outcome of the authentication) with respect to the initialization key**[78].

FIA_AFL.1.2/Init:

When the defined number of
Refinement: authentication attempts
has been **met**[79], the TSF shall **block the initialization key**[80].

6.3.2 FIA_AFL.1/Pre-pers

Authentication failure handling in Step 6 "Pre-personalization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Pre-pers:

---

[73] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[74] [assignment: list of authentication events]
[75] [assignment: *met or surpassed*]
[76] [assignment: *list of actions*]
[77] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[78] [assignment: list of authentication events]
[79] [assignment: *met or surpassed*]
[80] [assignment: *list of actions*]

The TSF shall detect when **3**[81] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the Pre-personalization key**[82].

FIA_AFL.1.2/Pre-pers:

When the defined number of consecutive unsuccessful authentication attempts has been **met**[83], the TSF shall **block the Pre-personalization key**[84].

6.3.3 FIA_AFL.1/Pers

Authentication failure handling in Step 7 "Personalization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Pers:

The TSF shall detect when **an administrator configurable positive integer within the range between 1 and 15**[85] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the Personalization key**[86].

FIA_AFL.1.2/Pers:

When the defined number of consecutive unsuccessful authentication attempts has been **met**[87], the TSF shall **block the Personalization key**[88].

---

[81] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[82] [assignment: list of authentication events]
[83] [assignment: *met or surpassed*]
[84] [assignment: *list of actions*]
[85] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[86] [assignment: list of authentication events]
[87] [assignment: *met or surpassed*]
[88] [assignment: *list of actions*]

6.3.4 FIA_AFL.1/PACE

Authentication failure handling – PACE authentication using non-blocking authorization data

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PACE:

The TSF shall detect when **an administrator configurable positive integer within 1 and 255**[89] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[90].

FIA_AFL.1.2/PACE:

When the defined number of consecutive unsuccessful authentication attempts has been met[91], the TSF shall **issue the result of the authentication with a few seconds delay**[92].

Application Note 59 *The count of consecutive unsuccessful authentications is stored in non-volatile memory and is preserved across power-up and power-down cycles. After a successful authentication, the count is reset to zero.*

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

6.3.5 FIA_UID.1/PACE

Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

[89] [assignment*: positive integer number*]
[90] [assignment: *list of authentication events*]
[91] [selection: *met*, *surpassed*]
[92] [assignment: *list of actions*]

FIA_UID.1.1/PACE:

The TSF shall allow

- to establish the communication channel,
- carrying out the PACE protocol according to [R23],
- to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
- to carry out the Chip Authentication Protocol v.1 according to [R13],
- to carry out the Terminal Authentication Protocol v.1 according to [R13][93],
- **to carry out the Active Authentication mechanism according to [R23]**[94]

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 60 *The SFR FIA_UID.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in the PACE PP [R12] by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 61 *After personalization in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization key).*

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

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

Application Note 62 *In Step 5, Initialization, of Phase 2, Manufacturing of the TOE, the Initialization Agent is the only user role known to the TOE which writes the Initialization Data in the audit records of the IC. The user in role Initialization Agent identifies himself by means of the GIM mechanism described in the initialization guidance. In Step 6, Pre-personalization, of Phase 2, Manufacturing of the TOE, the Pre-personalization Agent is the only user role known to the TOE which writes the Pre-personalization Data in the audit records of the IC. The Pre-personalization Agent creates the user role Personalization Agent for transition from Phase 2 to Phase 3, Personalization of the e-Document. The users in roles Pre-personalization Agent or Personalization Agent identify themselves by means of selecting the authentication key. After personalization in Phase 3, the PACE domain parameters, the Chip Authentication data, and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1, or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization key).*

Application Note 63 *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 e-Document holder itself or an authorised other person or device (Basic Inspection System with PACE).*

Application Note 64 *In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialization Data and/or the Pre-personalization Data in the audit records of the IC.*
Note that the Initialization Agent, the Pre-personalization Agent and the Personalization Agent act on behalf of the e-Document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for the Initialization Agent, the Pre-personalization Agent and the Personalization Agent. 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 roles Initialization Agent, Pre-personalization Agent or Personalization Agent, when a terminal proves the respective Terminal Authorization Level as defined by the related policy (policies).

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

6.3.6 FIA_UAU.1/PACE

Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/PACE:

The TSF shall allow

- to establish the communication channel,
- carrying out the PACE Protocol according to [R23],
- to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
- to identify themselves by selection of the authentication key,
- to carry out the Chip Authentication Protocol Version 1 according to [R13],
- to carry out the Terminal Authentication Protocol Version 1 according to [R13][95],
- **to carry out the Active Authentication mechanism according to [R23]**[96]

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

FIA_UAU.1.2/PACE:

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

Application Note 65 *The SFR FIA_UAU.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in the PACE PP [R12] by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 66 *The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable; i.e. it is either the e-Document holder itself or an authorised*

[95] [assignment: *list of TSF-mediated actions*]
[96] [assignment: *list of TSF-mediated actions*]

other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}), cf. FTP_ITC.1/PACE.

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

6.3.7 FIA_UAU.4/PACE

Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1/PACE:

The TSF shall prevent reuse of authentication data related to

- PACE Protocol according to [R23],
- Authentication Mechanisms based on **Triple-DES and AES**[97],
- Terminal Authentication Protocol v.1 according to [R13][98].

Application Note 67 *The SFR FIA_UAU.4.1 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] 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 [R12].*

Application Note 68 *The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. In addition, the authentication as Pre-personalization Agent or as Personalization Agent makes use of a diversifier, thus ensuring protection against replay attacks, such as the use of an internal counter as a diversifier. Observe that replay attacks cannot have any effect during Initialization, because they can only re-propose*

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

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

the same configuration data and the key retry counter is decreased even in case of success (cf. section 6.3.1).

Application Note 69 *Usage of the algorithm Triple-DES is deprecated.*

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

6.3.8 FIA_UAU.5/PACE

Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE:

The TSF shall provide

- PACE Protocol according to [R23],
- Passive Authentication according to [R23],
- Secure messaging in MAC-ENC mode according to [R23],
- Symmetric Authentication Mechanisms based on **Triple-DES and AES**[99],
- Terminal Authentication Protocol v.1 according to [R13][100]

to support user authentication.

FIA_UAU.5.2/PACE:

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

- Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging

[99] [selection: *Triple-DES, AES or other approved algorithms*]
[100] [assignment: *list of multiple authentication mechanism(s)*]

with the key agreed with the terminal by means of the PACE protocol.

- The TOE accepts the authentication attempt as Personalization Agent by **the Symmetric Authentication Mechanism based on Triple-DES with Personalization keys**[101].
- 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.
- 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[102]

Refinement: or the public key presented during PACE-CAM and the secure messaging established by PACE-CAM.

- **The TOE accepts the authentication attempt as Initialization Agent by the Symmetric Authentication Mechanism based on AES with Initialization keys**[104].
- **The TOE accepts the authentication attempt as Pre-personalization Agent by the Symmetric Authentication Mechanism based on Triple-DES with Pre-personalization keys**[105].

Application Note 70 *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 e-Document application.*

Application Note 71 *The Symmetric Authentication Mechanism for the Initialization Agent is based on AES, and uses a diversification algorithm as described in the initialization guidance.*

---

[101] [selection: *the Authentication Mechanism with Personalization keys*]
[102] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[103] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[104] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[105] [selection: *the Authentication Mechanism with Personalization keys*]

Application Note 72 *The Symmetric Authentication Mechanism for Pre-personalization Agent and Personalization Agent uses the CPS protocol [R20] based on Triple-DES. This mechanism uses a key diversification algorithm based on data randomly chosen by the card.*

Application Note 73 *The PACE protocol may use both Triple-DES and AES to encipher the random generated in step 1 of the protocol. However, usage of the algorithm Triple-DES is deprecated.*

Application Note 74 *The Embedded Software uses the symmetric co-processor provided by the platform to perform Triple-DES and AES.*

Application Note 75 *The SFR FIA_UAU.5.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.*

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

6.3.9 FIA_UAU.6/PACE

Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE:

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the PACE terminal[106].

Application Note 76 *The PACE protocol specified in [R23] 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*

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

incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

6.3.10 FIA_UAU.6/EAC/CAV1

Re-authenticating – Re-authenticating of Terminal by the TOE after Chip Authentication version 1

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[107].

6.3.11 FIA_UAU.6/EAC/CAM

Re-authenticating – Re-authenticating of Terminal by the TOE after PACE-CAM

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC/CAM:

The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of **PACE with Chip Authentication Mapping** shall be verified as being sent by the Inspection System[108].

Application Note 77 *The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [R23] 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*

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

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.

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

6.3.12 FIA_API.1/CAV1

Authentication Proof of Identity by Chip Authentication version 1

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CAV1:

The TSF shall provide Chip Authentication Protocol Version 1 according to [R23][109] to prove the identity of the TOE[110].

6.3.13 FIA_API.1/CAM

Authentication Proof of Identity by PACE with Chip Authentication Mapping

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CAM:

The TSF shall provide **PACE with Chip Authentication Mapping according to [R23]**[111] to prove the identity of the TOE[112].

[109] [assignment: *authentication mechanism*]
[110] [assignment: *authorized user or rule*]
[111] [assignment: *authentication mechanism*]
[112] [assignment: *authorized user or rule*]

Application Note 78 *FIA_API.1/CAV1 and FIA_API.1/CAM require the TOE to implement Chip Authentication by Chip Authentication Mechanism Version 1 specified in [R13]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [R23]. the terminal verifies by means of secure messaging whether the e-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).*

6.3.14 FIA_API.1/AA

Authentication Proof of Identity by Active Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA:

The TSF shall provide **Active Authentication Protocol according to [R23]**[113] to prove the identity of the **TOE**[114].

6.4 Class FDP: User data protection

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

6.4.1 FDP_ACC.1/TRM

Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/TRM:

[113] [assignment: *authentication mechanism*]

[114] [assignment: *authorized user or rule*]

The TSF shall enforce the Access Control SFP[115] on terminals gaining access to the User Data and data stored in EF.SOD of the logical e-Document[116].

Application Note 79 *The SFR FIA_ACC.1.1 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by data stored in EF.SOD of the logical e-Document. This extension does not conflict with the strict conformance to PACE PP.*

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

6.4.2 FDP_ACF.1/TRM

Security attribute based access control – Terminal Access

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/TRM:

The TSF shall enforce the Access Control SFP[117] to objects based on the following:

1. Subjects:
   a. Terminal,
   b. BIS-PACE,
   c. Extended Inspection System.
2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical e-Document,
   b. data in EF.DG3 of the logical e-Document,
   c. data in EF.DG4 of the logical e-Document,

[115] [assignment: *access control SFP*]
[116] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[117] [assignment: *access control SFP*]

d. all TOE intrinsic secret cryptographic keys stored in the e-Document[118].

3. Security attributes:

a. authentication status of terminals,

b. PACE Authentication,

c. Terminal Authentication v.1,

d. Authorization of the Terminal[119].

FDP_ACF.1.2/TRM:

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

- A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [R23] after a successful PACE authentication as required by FIA_UAU.1/PACE[120].

FDP_ACF.1.3/TRM:

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[121].

FDP_ACF.1.4/TRM:

The TSF shall explicitly deny access of subjects to objects based on the following rules:

- 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 e-Document.
- Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the e-Document.

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

[119] [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*]

[120] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations or controlled objects*]

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

- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
- Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
- Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
- Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4[122].

Application Note 80 *The read access to user data in the personalization phase is protected by a Restricted Application Secret Code.*

Application Note 81 *The SFR FDP_ACF.1.1/TRM in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [R12]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.*

Application Note 82 *The relative Certificate Holder Authorization encoded in the CV certificate of the inspection system is defined in [R14]. 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 83 *Please note that the Document Security Object (SO_D) stored in EF.SOD (see [R22]) 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 [R23].*

Application Note 84 *Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.*

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

The TOE shall meet the requirement “Subset residual information protection” (FDP_RIP.1) as specified below (Common Criteria Part 2).

6.4.3 FDP_RIP.1

Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1:

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from**[123] 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[124])[125].

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

6.4.4 FDP_UCT.1/TRM

Basic data exchange confidentiality – e-Document

Hierarchical to: No other components.

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

[123] [selection: *allocation of the resource to, deallocation of the resource from*]
[124] According to [R23]
[125] [assignment: *list of objects*]

FDP_UCT.1.1/TRM:

The TSF shall enforce the Access Control SFP[126] to be able to transmit and receive[127] user data in a manner protected from unauthorized disclosure.

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

6.4.5 FDP_UIT.1/TRM

Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1/TRM:

The TSF shall enforce the Access Control SFP[128] to be able to transmit and receive[129] user data in a manner protected from modification, deletion, insertion and replay[130] errors.

FDP_UIT.1.2/TRM:

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[131] has occurred.

Application Note 85 *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 either after successful PACE-CAM or after successful*

[126] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[127] [selection: *transmit, receive*]
[128] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[129] [selection: *transmit, receive*]
[130] [selection: *modification, deletion, insertion, replay*]
[131] [selection: *modification, deletion, insertion, replay*]

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).

6.5 Class FTP: Trusted path/channels

6.5.1 FTP_ITC.1/PACE

Inter-TSF trusted channel after PACE or Chip Authentication

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 enforce communication via the trusted channel for any data exchange between the TOE and the Terminal[132].

Application Note 86 *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 is initiated by the Terminal, and the TOE enforces the trusted channel.*

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

Application Note 87 *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 session keys established after Chip Authentication, either as part of PACE-CAM or as Chip Authentication Protocol Version 1.*

Application Note 88 *Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.*

6.5.2 FTP_ITC.1/CPS

Inter-TSF trusted channel after CPS Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/CPS:

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/CPS:

The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/CPS:

The TSF shall enforce communication via the trusted channel for **any data exchange between the TOE and the Terminal in Pre-personalization and in Personalization**[133].

Application Note 89 *This SFR requires any data exchanged after a CPS authentication in Pre-personalization or in Personalization to be transmitted over a secured channel. In particular, Active Authentication data are transmitted through the secure channel established by the Pre-personalization Terminal.*

6.6 Class FMT: Security management

The SFRs FMT_SMF.1 and FMT_SMR.1 provide basic requirements on the management of the TSF data.

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

6.6.1 FMT_SMF.1

Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1:

The TSF shall be capable of performing the following security management functions:

- Initialization,
- Pre-Personalization,
- Personalization,
- Configuration[134].

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

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

Application Note 90 *The ability to initialize, personalize, and configure the TOE is restricted to a successfully authenticated Initialization Agent, Pre-personalization Agent or Personalization Agent by means of symmetric keys. Initialization key may be used with uninitialized products only. Pre-personalization keys are only active in initialized but not pre-personalized products. Personalization keys are only active in pre-personalized but not personalized products. The e-Document locks out after a programmable number of consecutive unsuccessful authentication attempts.*

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

6.6.2 FMT_SMR.1/PACE

Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/PACE:

The TSF shall maintain the roles

- Manufacturer,
- Personalization Agent,
- Terminal,
- PACE authenticated BIS-PACE,
- Country Verifying Certification Authority,
- Document Verifier,
- **Basic Inspection System**,
- Domestic Extended Inspection System,
- Foreign Extended Inspection System[135].

FMT_SMR.1.2/PACE:

The TSF shall be able to associate users with roles.

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

Application Note 91 *The SFR FMT_SMR.1.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.*

Application Note 92 *For explanation on the role Manufacturer and Personalization Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the e-Document presenter).*

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

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

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

6.6.3 FMT_LIM.1

Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1:

The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow:

- User Data to be disclosed or manipulated,
- TSF data to be disclosed or manipulated,
- software to be reconstructed,
- substantial information about construction of TSF to be gathered which may enable other attacks, and

- sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[136].

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

6.6.4 FMT_LIM.2

Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1:

The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow:

- User Data to be disclosed or manipulated,
- TSF data to be disclosed or manipulated,
- software to be reconstructed,
- substantial information about construction of TSF to be gathered which may enable other attacks, and
- sensitive User Data (EF.DG3 and EF.DG4) to be disclosed[137].

Application Note 93 *The formulation of “Deploying Test Features …” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless, the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*
Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

[136] [assignment: *limited capability and availability policy*]
[137] [assignment: *limited capability and availability policy*]

Application Note 94 *The following SFRs are iterations of the component "Management of TSF data" (FMT_MTD.1). The TSF data include, but are not limited to, those identified below.*

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

6.6.5 FMT_MTD.1/INI_ENA

Management of TSF data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA:

The TSF shall restrict the ability to write[138] the Initialization Data and Pre-personalization Data[139] to the Manufacturer[140].

Application Note 95 *IC Initialization Data are written by the IC Manufacturer, TOE Initialization Data are written by the Initialization Agent, and Pre-personalization Data are written by the Pre-personalization Agent, according to the life cycle described in section 1.5. The IC Initialization Data include the Initialization key, the TOE Initialization Data include the Pre-personalization keys.*

6.6.6 FMT_MTD.1/INI_DIS

Management of TSF data – Reading and Using Initialization and Pre-personalization Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

[138] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[139] [assignment: *list of TSF data*]
[140] [assignment: *the authorised identified roles*]

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS:

The TSF shall restrict the ability to read out[141] the Initialization Data and the Pre-personalization Data[142] to the Personalization Agent[143]

6.6.7 FMT_MTD.1/CVCA_INI

Management of TSF data – Initialization of CVCA Certificate and Current Date

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_INI:

The TSF shall restrict the ability to write[144] the

- initial Country Verifying Certification Authority Public Key,
- initial Country Verifying Certification Authority Certificate,
- initial Current Date[145]

to **the Personalization Agent**[146].

Application Note 96 *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [R14]). 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 are needed for verification of the certificates and the calculation of the Terminal Authorization.*

[141] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[142] [assignment: *list of TSF data*]
[143] [assignment: *the authorised identified roles*]
[144] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[145] [assignment: *list of TSF data*]
[146] [assignment: *the authorised identified roles*]

6.6.8 FMT_MTD.1/CVCA_UPD

Management of TSF data – Country Verifying Certification Authority

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CVCA_UPD:

The TSF shall restrict the ability to update[147] the

- Country Verifying Certification Authority Public Key,
- Country Verifying Certification Authority Certificate[148]

to Country Verifying Certification Authority[149].

Application Note 97 *The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA link certificates (cf. [R14]). 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. [R14]).*

6.6.9 FMT_MTD.1/DATE

Management of TSF data – Current date

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/DATE:

The TSF shall restrict the ability to modify[150] the Current Date[151] to

- Country Verifying Certification Authority,

[147] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[148] [assignment: *list of TSF data*]
[149] [assignment: *the authorised identified roles*]
[150] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[151] [assignment: *list of TSF data*]

- Document Verifier,
- Domestic Extended Inspection System[152].

Application Note 98 *The authorized roles are identified in their certificate (cf. [R14]) 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. [R14]).*

6.6.10 FMT_MTD.1/CAPK

Management of TSF data – Chip Authentication Private Key

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/CAPK:

The TSF shall restrict the ability to **load**[153] the Chip Authentication Private Key[154] to **the Pre-personalization Agent**[155].

Application Note 99 *The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.*

6.6.11 FMT_MTD.1/KEY_READ

Management of TSF data – Key Read

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

[152] [assignment: *the authorised identified roles*]
[153] [selection: *create, load*]
[154] [assignment: *list of TSF data*]
[155] [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ KEY_READ:

The TSF shall restrict the ability to read[156] the

- PACE passwords,
- Chip Authentication Private Key,
- Personalization keys[157],
- **Initialization key,**
- **Pre-personalization keys,**
- **Active Authentication Private Key.**

to none[158].

Application Note 100 *The SFR FMT_MTD.1/KEY_READ in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.*

6.6.12 FMT_MTD.1/PA

Management of TSF data – Personalization Agent

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/PA:

The TSF shall restrict the ability to write[159] the Document Security Object (SO_D)[160] to the Personalization Agent[161].

Application Note 101 *By writing SO_D into the TOE, the Personalization Agent confirms (on behalf of DS) the correctness of all the personalization data related. This consists of user- and TSF-data.*

---

[156] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[157] [assignment: *list of TSF data*]
[158] [assignment: *the authorised identified roles*]
[159] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[160] [assignment: *list of TSF data*]
[161] [assignment: *the authorised identified roles*]

6.6.13 FMT_MTD.1/AAPK

Management of TSF data – Active Authentication Private Key

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/AAPK:

The TSF shall restrict the ability to write[162] the **Active Authentication Private Key**[163] to **the Pre-personalization Agent** [164].

Application Note 102 *The addition of this SFR does not impair the conformance to the Protection Profiles.*

The TOE shall meet the requirement “Secure TSF data (FMT_MTD.3)” as specified below (Common Criteria Part 2).

6.6.14 FMT_MTD.3

Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1:

The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[165].

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

[162] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[163] [assignment: *list of TSF data*]
[164] [assignment: *the authorised identified roles*]
[165] [assignment: l*ist of TSF data*]

- **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,**
- **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,**
- **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 103 *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.*

6.7 Class FPT: Protection of the security functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF-data. 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.

The TOE shall meet the requirement "TOE emanation (FPT_EMS.1)" as specified below (Common Criteria Part 2 extended).

6.7.1 FPT_EMS.1

TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1:

The TOE shall not emit **electromagnetic and current emissions**[166] in excess of **intelligible threshold**[167] enabling access to

- Chip Authentication Session Keys,
- PACE Session Keys (PACE-K_{MAC}, PACE-K_{ENC}),
- the ephemeral private key ephem-SK_{PICC}-PACE,
- **Initialization key,**
- **Pre-personalization keys,**
- **Active Authentication Private Key**[168],
- Personalization keys,
- Chip Authentication Private Key[169], and
- **EF.DG1 to EF.DG16, EF.SOD, EF.COM**[170].

FPT_EMS.1.2:

[166] [assignment: *type of emissions*]
[167] [assignment: *specified limits*]
[168] [assignment: *list of types of TSF data*]
[169] [assignment: *list of types of TSF data*]
[170] [assignment: *list of types of user data*]

The TSF shall ensure any users[171] are unable to use the following interface smart card circuits contacts[172] to gain access to

- Chip Authentication Session Keys,
- PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),
- the ephemeral private key ephem-SK_{PICC}-PACE,
- **Initialization key,**
- **Pre-personalization keys,**
- **Active Authentication Private Key**[173],
- Personalization keys,
- Chip Authentication Private Key[174], and
- **EF.DG1 to EF.DG16, EF.SOD, EF.COM**[175].

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

Application Note 104 *The SFR FPT_EMS.1.1 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [7] by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.*

Application Note 105 *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The e-Document's chip can provide a smart card contactless interface according to ISO/IEC 14443 [R31] [R32] and contact based*

[171] [assignment: *type of users*]
[172] [assignment: *type of connection*]
[173] [assignment: *list of types of TSF data*]
[174] [assignment: *list of types of TSF data*]
[175] [assignment: *list of types of user data*]

interface according to ISO/IEC 7816-2 [R28] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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

6.7.2 FPT_FLS.1

Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1:

The TSF shall preserve a secure state when the following types of failures occur:

- exposure to operating conditions causing a TOE malfunction,
- failure detected by TSF according to FPT_TST.1[176].

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

6.7.3 FPT_TST.1

TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

FPT_TST.1.1:

The TSF shall run a suite of self-tests **during initial start-up**[177]**, and at the conditions: before any use of TSF data**[178] to demonstrate the correct operation of the TSF[179].

FPT_TST.1.2:

The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[180].

FPT_TST.1.3:

The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[181].

Application Note 106 *A dedicated software in the protected ROM of the IC S3D350A (rev2) provides full test capabilities (operating system for test, "OST"), not accessible by the Security IC Embedded Software after delivery.*

Application Note 107 *At start-up, the OS checks whether a reset has been triggered by a sensor. If this is the case, a reset counter is incremented. If the count exceeds 32, then the chip is irreversibly blocked. Before any read of the TSF data, the EEPROM memory is checked for possible fault injection events. If this is the case, the reset counter is incremented and the chip goes into an endless loop. During normal operation, tests of the random number generation and integrity checks are also executed.*

Application Note 108 *FPT_TST.1.3 protects the integrity of the code by physical means, using the mechanisms of the underlying IC. After delivery, the TOE does not use logical means to check the integrity of the code, as it relies on the IC security features to provide verification of the code integrity.*

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

---

[177] [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]*]
[178] [*assignment: conditions under which self test should occur*]
[179] [selection: *[assignment: parts of TSF], the TSF*]
[180] [selection: *[assignment: parts of TSF], TSF data*]
[181] [selection: *[assignment: parts of TSF], TSF*]

6.7.4 FPT_PHP.3

Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1:

The TSF shall resist physical manipulation and physical probing[182] to the TSF[183] by responding automatically such that the SFRs are always enforced.

Application Note 109 *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.*

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

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

7. Security assurance requirements

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5), augmented by taking the components ALC_DVS.2 and AVA_VAN.5.

Table 7-1 summarizes the assurance components that define the security assurance requirements for the TOE.

Table 7-1 Assurance requirements at EAL5+

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

Application Note 110 *The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using either PACE-CAM or Chip Authentication Protocol v.1 (OE.Prot_Logical_e-Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).*

8. Security requirements rationale

8.1 Security functional requirements rationale

Table 8-1 provides an overview for security functional requirements coverage of security objectives.

Table 8-1 Coverage of security objectives for the TOE by SFRs

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	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	X				X					
FCS_CKM.1/GIM				X			X								
FCS_CKM.1/CPS					X	X	X	X							
FCS_CKM.1/DH_PACE							X	X	X						
FCS_CKM.1/CA	X	X					X	X	X						
FCS_CKM.4	X				X	X	X	X	X						
FCS_COP.1/AUTH				X	X	X									
FCS_COP.1/AA_SIGN			X					X							
FCS_COP.1/PACE_ENC									X						
FCS_COP.1/CA_ENC	X	X			X	X	X		X						
FCS_COP.1/PACE_MAC							X	X							
FCS_COP.1/CA_MAC	X	X			X	X	X								
FCS_COP.1/SIG_VER	X														
FCS_RND.1	X				X	X	X	X	X						
FIA_AFL.1/Init				X									X		
FIA_AFL.1/Pre-pers													X		
FIA_AFL.1/Pers													X		
FIA_AFL.1/PACE													X		
FIA_UID.1/PACE	X			X	X	X	X	X	X						
FIA_UAU.1/PACE	X			X	X	X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X	X	X						
FIA_UAU.5/PACE	X			X	X	X	X	X	X						
FIA_UAU.6/PACE							X	X	X						
FIA_UAU.6/EAC/CAV1	X						X	X	X						
FIA_UAU.6/EAC/CAM	X						X	X	X						
FIA_API.1/CAV1		X													
FIA_API.1/CAM		X													
FIA_API.1/AA			X												

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	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
FDP_ACC.1/TRM	X			X	X	X	X		X						
FDP_ACF.1/TRM	X			X	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		
FTP_ITC.1/CPS							X	X	X						
FMT_SMF.1		X		X	X	X	X	X	X	X					
FMT_SMR.1/PACE		X		X	X	X	X	X	X	X					
FMT_LIM.1											X				
FMT_LIM.2											X				
FMT_MTD.1/INI_ENA				X	X	X				X					
FMT_MTD.1/INI_DIS						X				X					
FMT_MTD.1/CVCA_INI	X														
FMT_MTD.1/CVCA_UPD	X														
FMT_MTD.1/DATE	X														
FMT_MTD.1/CAPK	X	X					X								
FMT_MTD.1/PA						X	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X	X	X	X	X	X	X						
FMT_MTD.1/AAPK			X				X								
FMT_MTD.3	X														
FPT_EMS.1				X	X	X						X			
FPT_TST.1												X			X
FPT_FLS.1												X			X
FPT_PHP.3							X					X		X	

The security objective **OT.Identification** “Identification of the TOE” addresses the storage of Initialization 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 Initialization and Pre-personalization Data (including the Personalization key). The SFR ***FMT_MTD.1/INI_DIS*** requires the Personalization Agent to disable access to Initialization and Pre-personalization Data in the life cycle phase ‘operational use’. The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related.

The security objective **OT.AC_Init**, Access Control for Initialization of logical e-Document, addresses the access control of the writing the logical e-Document in Step 5, Initialization. The Initialization Agent is authenticated by decrypting the initialization cryptograms using a mechanism based on AES as described in the initialization guidance (***FCS_COP.1/AUTH***) with the Initialization key (***FCS_CKM.1/GIM***). The authentication failures are managed according to ***FIA_AFL.1/Init***.
The authentication of the terminal as Initialization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4/PACE*** and ***FIA_UAU.5/PACE***.
The justification for the SFRs ***FAU_SAS.1*** and ***FMT_MTD.1/INI_ENA*** arises from the justification for **OT.Identification** above with respect to the Initialization Data. The write access to the logical e-Document data is defined by the SFRs ***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 Initialization Agent is allowed to write the OS configuration data. The SFR ***FMT_SMR.1/PACE*** lists the roles (including Initialization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Initialization). The SFRs ***FMT_MTD.1/KEY_READ*** and ***FPT_EMS.1*** restrict the access to the Initialization key.

The security objective **OT.AC_Pre-pers** “Access Control for Pre-personalization of logical e-Document” addresses the access control of the writing the logical e-Document in Step 6 “Pre-personalization”. The Pre-personalization Agent is authenticated by using the CPS mechanism based on Triple-DES (***FCS_CKM.1/CPS***, ***FCS_COP.1/AUTH***, and ***FCS_RND.1*** for key generation) with the Pre-personalization keys by using the CPS mechanism. The authentication of the terminal as Pre-personalization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4/PACE*** and ***FIA_UAU.5/PACE***. If the Pre-personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Pre-personalization key, the TOE will use the TSF according to ***FCS_RND.1*** (for the generation of the challenge), ***FCS_COP.1/CA_ENC*** (to verify the authentication attempt and for secure messaging), 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 justification for the SFRs ***FAU_SAS.1*** and ***FMT_MTD.1/INI_ENA*** arises from the justification for **OT.Identification** above with respect to the Pre-personalization Data. The write access to the logical e-Document data is defined by the SFRs ***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 Pre-personalization Agent is allowed to write the data of the groups EF.DG14, EF.DG15 of the logical e-Document. The SFR ***FMT_SMR.1/PACE*** lists the roles (including Pre-personalization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Pre-personalization). The SFRs ***FMT_MTD.1/KEY_READ*** and ***FPT_EMS.1*** restrict the access to the Personalization keys, the Chip Authentication Private Key, the PACE passwords, and the Active Authentication key.

The security objective **OT.AC_Pers** “Access Control for Personalization of logical e-Document” addresses the access control of the writing the logical e-Document. The Personalization Agent is authenticated by using the CPS mechanism based on Triple-DES

(***FCS_CKM.1/CPS***, ***FCS_COP.1/AUTH***, and ***FCS_RND.1*** for key generation), with the Personalization keys by using the CPS mechanism. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4/PACE*** and ***FIA_UAU.5/PACE***. 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 the TSF according to ***FCS_RND.1*** (for the generation of the challenge), ***FCS_COP.1/CA_ENC*** (to verify the authentication attempt and for secure messaging), 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 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 e-Document data is defined by the SFRs ***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 e-Document. ***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 keys, the Chip Authentication Private Key, the PACE passwords, and the Active Authentication key.

Application Note 111 *The Personalization Agent can authenticate itself using the symmetric authentication mechanism only. No other authentication mechanism is available to the Personalization Agent.*

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical e-Document stored on the e-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*** and ***FDP_ACF.1/TRM***: only the Pre-personalization Agent or the Personalization Agent are allowed to write the data in EF.DG1 to EF.DG16 of the logical e-Document of the logical e-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 e-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. The Pre-personalization Agent must identify and authenticate themselves according to ***FIA_UID.1/PACE*** and ***FIA_UAU.1/PACE*** before accessing data in Step 6 “Pre-personalization”. ***FIA_UAU.4/PACE***, ***FIA_UAU.5/PACE***, and ***FCS_CKM.4*** represent some required specific properties of the protocols used. The SFR

FMT_SMR.1/PACE lists the roles and the SFR ***FMT_SMF.1*** lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, in Pre-personalization and Personalization by ***FTP_ITC.1/CPS***, and in the Operational Use phase by **FDP_UCT.1/TRM,** **FDP_UIT.1/TRM** and ***FTP_ITC.1/PACE*** using ***FCS_COP.1/PACE_MAC*** for PACE. For secured data exchange in Initialization, a prerequisite is an authentication using an Initialization Key generated by the TOE (***FCS_CKM.1/GIM***). For secured data exchange in Pre-personalization and in Personalization, a prerequisite for establishing this trusted channel is a successful CPS Authentication using ***FCS_CKM.1/CPS***. 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/CAV1***, ***FIA_UAU.6/EAC/CAM***. 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 e-Document data after Chip Authentication v.1. The SFRs ***FIA_UAU.6/EAC/CAV1***, ***FIA_UAU.6/EAC/CAM***, and ***FDP_UIT.1/TRM*** require the integrity protection of the transmitted data after Chip Authentication performed either as part of PACE-CAM or as 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***, ***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***, and ***FMT_MTD.1/KEY_READ*** require that the Chip Authentication Key and Active Authentication key cannot be written unauthorized or read afterwards. The SFR ***FCS_RND.1*** represents a general support for cryptographic operations needed.

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 (PACE) and by an active verification by the TOE itself (PACE and Active Authentication).
This objective is mainly achieved by ***FTP_ITC.1/PACE*** using ***FCS_COP.1/PACE_MAC***, as well as ***FTP_ITC.1/CPS***. A prerequisite for establishing the trusted channel in the Operational Use phase 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/CAV1***, ***FIA_UAU.6/EAC/CAM***. A prerequisite for

establishing the trusted channel in Pre-personalization and in Personalization is a successful CPS authentication using ***FCS_CKM.1/CPS***. ***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.
The security objective **OT.Data_Authenticity** is also achieved by ***FCS_COP.1/AA_SIGN***.

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*** and ***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***, as well as by ***FTP_ITC.1/CPS***. 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/CAV1***, ***FIA_UAU.6/EAC/CAM***. ***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 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 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.

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

The SFRs ***FIA_UID.1/PACE*** and ***FIA_UAU.1/PACE*** require the identification and authentication of the inspection systems. The SFR ***FIA_UAU.5/PACE*** requires the

successful Chip Authentication (CA) performed as part of PACE-CAM or as Chip Authentication Protocol v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA, the reuse of authentication data is prevented by ***FIA_UAU.4/PACE***. The SFRs ***FIA_UAU.6/EAC/CAV1***, ***FIA_UAU.6/EAC/CAM***, and ***FDP_UCT.1/TRM*** requires 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***, ***FCS_COP.1/CA_MAC*** (for ENC_MAC_Mode secure messaging). The session keys are destroyed according to ***FCS_CKM.4*** after use. The SFRs ***FMT_MTD.1/CAPK*** and ***FMT_MTD.1/KEY_READ*** require 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 updated by authorized identified role as of ***FMT_MTD.1/CVCA_INI***, ***FMT_MTD.1/CVCA_UPD***, and ***FMT_MTD.1/DATE***.

The security objective **OT.Chip_Auth_Proof** "Proof of e-Document's chip authenticity" is ensured by the Chip Authentication provided by ***FIA_API.1/CAV1*** or ***FIA_API.1/CAM*** (depending on the Chip Authentication protocol used) 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***. Chip Authentication, performed as part of PACE-CAM [R23] or by Chip Authentication Protocol v.1 [R13], requires additional TSF according to ***FCS_CKM.1/CA*** (for the derivation of the session keys) and ***FCS_COP.1/CA_ENC***, ***FCS_COP.1/CA_MAC*** (for the ENC_MAC_Mode secure messaging).
The SFRs ***FMT_SMF.1*** and ***FMT_SMR.1/PACE*** support the functions and roles related.

The security objective **OT.Active_Auth_Proof** "Proof of e-Document's chip authenticity" is ensured by the Active Authentication Mechanism [R23] provided by ***FIA_API.1/AA***, proving the identity of the TOE. The Active Authentication Protocol defined by ***FIA_API.1/AA*** is performed using a TOE internally stored confidential private key as required by ***FMT_MTD.1/AAPK*** and ***FMT_MTD.1/KEY_READ***. This key is written to the TOE as defined by ***FMT_MTD.1/AAPK***. The Active Authentication Protocol requires additional TSF according to ***FCS_COP.1/AA_SIG*** (for the digital signature of Active Authentication data).

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

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the e-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 SFRs ***FPT_FLS.1*** and ***FPT_TST.1***, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR ***FPT_PHP.3***.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the e-Document directly through establishing a communication via the contact interface, or remotely through establishing or listening to a communication via the contactless interface of the TOE, without a priori knowledge of the correct values of the shared authentication data (Initialization key, Pre-personalization keys, Personalization keys, PACE passwords). This objective is achieved as follows:

- while establishing communication in pre-operational phases by ***FIA_AFL.1/Init, FIA_AFL.1/Pre-pers, FIA_AFL.1/Pers***;
- while establishing PACE communication with a PACE password, e.g. CAN or MRZ (non-blocking authorization data) – by ***FIA_AFL.1/PACE***;
- for listening to PACE communication (of importance for the current ST, since SO_D is card-individual) – by ***FTP_ITC.1/PACE***.

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

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

8.2 Dependency rationale

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

Table 8-2 shows the dependencies between the SFRs of the TOE.

Table 8-2 Dependencies between the SFRs for the TOE

SFR	Dependencies	Support of the dependencies
FAU_SAS.1	No dependencies	-
FCS_CKM.1/GIM	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/AUTH Fulfilled by FCS_CKM.4
FCS_CKM.1/CPS	[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, FCS_COP.1/CA_MAC Fulfilled by FCS_CKM.4
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, 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, FCS_COP.1/CA_MAC Fulfilled by FCS_CKM.4
FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/CPS, FCS_CKM.1/GIM
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	*Justification 3 for non-satisfied dependencies* *Justification 3 for non-satisfied dependencies*
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 2 for non-satisfied dependencies* *Justification 2 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

SFR	Dependencies	Support of the dependencies
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 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	-
FIA_AFL.1/Init	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/Pre-pers	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/Pers	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	-
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	-
FIA_UAU.5/PACE	No dependencies	-
FIA_UAU.6/PACE	No dependencies	-
FIA_UAU.6/EAC/CAV1	No dependencies	-
FIA_UAU.6/EAC/CAM	No dependencies	-
FIA_API.1/CAV1	No dependencies	-
FIA_API.1/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 1 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 or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	-
FTP_ITC.1/CPS	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

SFR	Dependencies	Support of the dependencies
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1/CVCA_INI, 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	-

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

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

Justification 2: Since AA does not provide for the generation or destruction of cryptographic keys, neither the SFR FCS_CKM.1 nor the SFR FCS_CKM.4 apply. The S3D350A (rev2) platform provides for ECDSA cryptographic library functions.

Justification 3: The SFR FCS_COP.1/AUTH refers to the symmetric Initialization Key, Pre-personalization Key and Personalization Key permanently stored, respectively, during IC manufacturing, initialization, and pre-personalization (cf. FMT_MTD.1/INI_ENA) by the Manufacturer. Thus, there is no necessity to generate or import these keys during the addressed TOE life cycle by the means of FCS_CKM.1 or FDP_ITC. Since these keys are permanently stored within the TOE, there is no need for FCS_CKM.4, too.

8.3 Security assurance requirements rationale

The 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 applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

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 fulfil the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies on other assurance requirements.

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

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

8.4 Security requirements – Mutual support and internal consistency

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

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

The dependency analysis in section 8.2 "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 analysed, and non-satisfied dependencies are appropriately explained.

All subjects and objects addressed by more than one SFR in section 6 "Security functional requirements" are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these "shared" items.

The assurance class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 8.3 "Security assurance requirements rationale" shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional assurance dependencies which are not met, a possibility which has been shown not to arise in section 8.2 "Dependency rationale" and 8.3 "Security assurance requirements rationale". Furthermore, as also discussed in section 8.3 "Security assurance requirements rationale", the chosen assurance components are adequate for the functionality of the TOE. Therefore, the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

9. TOE summary specification

9.1 Coverage of SFRs

Table 9-1 describes how each security functional requirement claimed in this security target is satisfied by the TOE.

Table 9-1 Implementation of the security functional requirements in the TOE

Security functional requirement	Implementation
FAU_SAS.1	The Manufacturer stores IC identification data in the audit records.
FCS_CKM.1/GIM	The TOE generates the 256-bit AES key for the authentication of the Initialization Agent. To this end, the TOE uses a key diversifier algorithm over a base key stored on the chip. The Initialization Key is used later for decrypting the Initialization Cryptogram. See Application Note 34
FCS_CKM.1/CPS	The TOE generates session keys for Secure Messaging soon after a successful CPS authentication of the Pre-personalization Agent or the Personalization Agent, as described in section 5.2 of EMV specification [R20]. See Application Note 33.
FCS_CKM.1/DH_PACE	The TOE generates session keys for Secure Messaging soon after a successful PACE or PACE-CAM authentication of the inspection terminal. See Application Note 34, Application Note 35 and Application Note 36
FCS_CKM.1/CA	The TOE generates session keys for Secure Messaging soon after a successful Chip Authentication v1 of the inspection terminal. See Application Note 37, Application Note 38, Application Note 39, Application Note 40, Application Note 41 and Application Note 42.
FCS_CKM.4	Session keys are overwritten with zeros when a Secure Messaging session is closed. See Application Note 43.

Security functional requirement	Implementation
FCS_COP.1/PACE_ENC	During a Secure Messaging session after a PACE authentication, the TOE encrypts transmitted data to ensure confidentiality, and decrypts received data, to restore original content. To this end, the TOE uses Triple-DES in CBC mode with 112-bit session key or AES with 128, 192 or 256 bit keys. See Application Note 48 and Application Note 49.
FCS_COP.1/PACE_MAC	During a Secure Messaging session after a PACE authentication, the TOE computes a Message Authentication Code (MAC) to check integrity of received data, and to allow integrity check by the terminal. The MAC computation is performed according to CMAC or Retail MAC algorithm and cryptographic key sizes 112, 128, 192 or 256 bits. See Application Note 50.
FCS_COP.1/CA_ENC	During a Secure Messaging session after a PACE-CAM or Chip Authentication v1, the TOE encrypts transmitted data to ensure confidentiality, and decrypts received data, to restore original content. To this end, the TOE uses Triple-DES in CBC mode with 112-bit session key or AES with 128, 192 or 256 bit keys. See Application Note 51 and Application Note 52.
FCS_COP.1/CA_MAC	During a Secure Messaging session after a PACE-CAM authentication or Chip Authentication v1, the TOE computes a Message Authentication Code (MAC) to check integrity of received data, and to allow integrity check by the terminal. The MAC computation is performed according to CMAC or Retail MAC algorithm and cryptographic key sizes 112, 128, 192 or 256 bits. See Application Note 53.
FCS_COP.1/SIG_VER	The TOE performs signature verification for Terminal Authentication using the ECDSA algorithm. See Application Note 54, Application Note 55 and Application Note 56.
FCS_COP.1/AA_SIGN	The TOE performs signature for Active Authentication using the ECDSA cryptography. See Application Note 46 and Application Note 47.

Security functional requirement	Implementation
FCS_COP.1/AUTH	The TOE provides a mechanism to authenticate the Pre-personalization Agent and the Personalization Agent. To this end, the TOE adopts the CPS protocol described in sections 4.1, 5.2 of [R20], using the Triple-DES in CBC mode with 112-bit Pre-personalization keys, and 112-bit Personalization keys. See Application Note 44 and Application Note 45.
FCS_RND.1	The TOE generates random numbers for use in the authentication protocols. See Application Note 57 and Application Note 58.
FIA_AFL.1/Init	In case of unsuccessful authentication, the Initialization Agent has only a limited number of authentication attempts after which the Initialization Key is blocked. The maximum number of consecutive failures is set to 31.
FIA_AFL.1/Pre-pers	In case of unsuccessful authentication, the Pre-personalization Agent has only a limited number of authentication attempts after which the Pre-personalization keys are blocked. The maximum number of consecutive failures is set by the actor that writes the Pre-personalization keys, i.e. the Initialization Agent.
FIA_AFL.1/Pers	In case of unsuccessful authentication, the Pre-personalization Agent has only a limited number of authentication attempts after which the Personalization keys are blocked. The maximum number of consecutive failures is set by the actor that writes the Personalization keys, i.e. the Pre-personalization Agent.
FIA_AFL.1/PACE	In case of unsuccessful PACE authentication, the TOE sends its response with an increasing delay to counter brute force attacks. The applied delay is set by the actor that writes the e-Document PACE key objects. See Application Note 59.

Security functional requirement	Implementation
FIA_UID.1/PACE	The TOE applies access control policies to guarantee that the following actions can be performed before the user is identified: • Establishment of a secure communication channel, • PACE authentication • Read access to the initialization data • Chip Authentication (as CA v1 or as parto of PACE-CAM), • Terminal Authentication, • Active Authentication. Any other action is forbidden without prior user identification. The required access privileges are set for each data set by the agent that writes the related persistent object. See Application Note 60, Application Note 61, Application Note 62, Application Note 63 and Application Note 64.
FIA_UAU.1/PACE	The TOE applies access control policies to guarantee that the following actions can be performed before the user is authenticated: • Establishment of a secure communication channel, • PACE authentication • Read access to the initialization data • Chip Authentication (as CA v1 or as parto of PACE-CAM), • Terminal Authentication, • Active Authentication. Any other action is forbidden without prior user authentication. The required access privileges are set for each data set by the agent that writes the related persistent object. See Application Note 65 and Application Note 66.
FIA_UAU.4/PACE	In case of unsuccessful authentication attempts, the TOE closes the current session, overwrites session keys with zeros and stops any further communication with the terminal. See Application Note 67, Application Note 68 and Application Note 69.

Security functional requirement	Implementation
FIA_UAU.5/PACE	The TOE provides: • the PACE mechanism to authenticate the user in the operational use, • the CPS mechanism to authenticate the Pre-personalization agent, • the CPS mechanism to authenticate the Pre-personalization agent, • Passive authentication to verify integrity of logical user data, • Secure Messaging in MAC-ENC mode, to guarantee confidentiality and integrity of data exchanged over a communication channel, • Terminal Authentication as final part of the EAC v1 mechanism. See Application Note 70, Application Note 72, Application Note 72, Application Note 73, Application Note 74 and Application Note 75.
FIA_UAU.6/EAC/CAV1	Secure Messaging established after a successful Chip Authentication v1 provides re-authentication of the user.
FIA_UAU.6/EAC/CAM	Secure Messaging established after a successful PACE-CAM authentication provides re-authentication of the user. See Application Note 78.
FIA_UAU.6/PACE	Secure Messaging established after a successful PACE authentication allows re-authentication of the user. See Application Note 76.
FIA_API.1/CAV1	The TOE proves the genuinity of the chip by performing Chip Authentication v1. Other methods to achieve that proof are described below for FIA_API.1/CAM and FIA_API.1/AA.
FIA_API.1/CAM	The TOE proves the genuinity of the chip by performing Chip Authentication as part of PACE-CAM. Other methods to achieve that proof are described below for FIA_API.1/CAV1 and FIA_API.1/AA. See Application Note 79.
FIA_API.1/AA	The TOE proves the genuinity of the chip by performing Active Authentication. Other methods to achieve that proof are described below for FIA_API.1/CAM and FIA_API.1/CAV1.

Security functional requirement	Implementation
FDP_ACC.1/TRM	The TOE applies an Access Control Policy to check that terminals wanting to access protected data possess the required privileges and have successfully completed the required authentication. The TSF checks the possess of the above requirements before any access to protected data. See Application Note 79.
FDP_ACF.1/TRM	The TOE keeps a security status for each of the data object related to the protected data listed in this SFR to guarantee entitlement to read and/or write those data. The TSF checks the security status is checked before any access to the protected data.
FDP_UCT.1/TRM	The TOE protects data confidentiality of received and transmitted data by means of Triple-DES or AES cryptography within Secure Messaging sessions in MAC-ENC mode.
FDP_UIT.1/TRM	The TOE guarantees data integrity by means of a Message Authentication Code (MAC) within Secure Messaging sessions in MAC-ENC mode. The MAC: • is computed on data to be transmitted and sent to the terminal together with the data and is checked upon data reception to allow tampering detection. See Application Note 85.
FDP_RIP.1	The TOE clears session keys and private ephemeral keys by overwriting them with zeors. The TOE also clears the context under witch those keys have been used.
FTP_ITC.1/PACE	After PACE or Chip Authentication the TOE establishes a secure channel with the terminal (the trusted IT product). After that, all data are exchanged in Secure Messaging in ENC_MAC mode. Therefore, confidentiality is protected by encryption and checking of MAC allows tampering detection. See Application Note 86, Application Note 87 and Application Note 88.
FTP_ITC.1/CPS	After PACE or Chip Authentication the TOE establishes a secure channel with the terminal (the trusted IT product). After that, all data are exchanged in Secure Messaging in ENC_MAC mode. Therefore, confidentiality is protected by encryption and checking of MAC allows tampering detection. See Application Note 89.

Security functional requirement	Implementation
FMT_SMF.1	The TOE provides features for storing Initialization data, Pre-personalization Data and Personalization Data, ensuring that only the entitled agents are able to do so. See Application Note 90
FMT_SMR.1/PACE	The TOE distinguishes between the roles IC Manufacturer, Pre-personalization Agent, Personalization Agent, Terminal, PACE-authenticated Basic Inspection System, CVCA, Document Verifier, Basic Inspection System, Domestic and Foreign Extended Inspection System. All these roles are granted the access privileges allowed by the security policies and are implicitly identified via the corresponding authentication key. See Application Note 91 and Application Note 92.
FMT_LIM.1	The test features of the OS, as well as the authentication mechanism granting access to them, are permanently disabled in the evaluated configuration of the OS. As regards the test features of the IC, information on their limitation is provided in the TOE summary specification of the public security target of the supported IC for platform SFRs FMT_LIM.1, FMT_LIM.2 [R40].
FMT_LIM.2	As specified for SFR FMT_LIM.1.
FMT_MTD.1/INI_ENA	The access control policy enforced by the TOE guarantees that in the Initialization and Pre-personalization phases only the entitled agents can write data. The TSF checks the possess of access privileges before any access is made. See Application Note 95.
FMT_MTD.1/INI_DIS	The access control policy enforced by the TOE guarantees that initialization data can be read by the Personalization Agent only. The TSF checks the possess of access privileges before any access is made to those data.
FMT_MTD.1/CVCA_INI	The access control policy enforced by the TOE guarantees that CVCA public and private keys, as well as current data can be written by the Personalization Agent only. The TSF checks the possess of access privileges before any access is made to those data. See Application Note 96.

Security functional requirement	Implementation
FMT_MTD.1/CVCA_UPD	The access control policy enforced by the TOE guarantees that CVCA public and private keys can be updated by the CVCA only. The TSF checks the possess of access privileges before any access is made to those data. See Application Note 97.
FMT_MTD.1/DATE	The access control policy enforced by the TOE guarantees that the current data can be updated by the CVCA, or DV or Domestic EIS only. The TSF checks the possess of access privileges before any access is made to those data. See Application Note 98.
FMT_MTD.1/CAPK	The access control policy enforced by the TOE guarantees that the Chip Authentication private key can be loaded by the Pre-personalization Agent only. The TSF checks the possess of access privileges before any access is made to those data. See Application Note 99.
FMT_MTD.1/KEY_READ	The property defining read access conditions of: • PACE passwords, • Chip Authentication private key, • Pre-personalizaton keys, • Personalization keys, • Active Authentication private key are set, when those keys are written, so that the keys cannot be read by no one under any circumstances. The TSF checks the access privileges before any access is made to those keys. See Application Note 100.
FMT_MTD.1/PA	The property defining read access conditions of: • PACE passwords, • Chip Authentication private key, • Pre-personalizaton keys, • Personalization keys, • Active Authentication private key are set, when those keys are written, so that the keys cannot be read by no one under any circumstances. The TSF checks the access privileges before any access is made to those keys. See Application Note 101.

Security functional requirement	Implementation
FMT_MTD.1/AAPK	The access control policy enforced by the TOE guarantees that the Active Authentication private key can be written by the Pre-personalization Agent only. The TSF checks the possess of access privileges before any access is made to those data. See Application Note 102.
FMT_MTD.3	The TSF checks the security and the validity of values in the certificate chain before using those data for Terminal Authentication and Access Control mechanisms. See Application Note 103.
FPT_EMS.1	Leakage of confidential data through side channels is prevented by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [R41][R42][R43].
FPT_FLS.1	In case self-test fails or a physical attack is detected, the OS enters an endless loop, so that all cryptographic operations and data output interfaces are inhibited.
FPT_TST.1	During initial start-up, the IC performs a self-test procedure that tests alarm lines and environmental sensor mechanisms (cf. [R41]), and the OS checks the integrity of the TSF by computing a hash value of the code and comparing it with a reference hash value stored internally. Moreover, the integrity of TSF data is checked whenever they are used. In case any one of such checks fails, the OS enters an endless loop, so that the resulting fall of communication informs the user about the integrity error. See also Application Note 106, Application Note 107 and Application Note 108.
FPT_PHP.3	Detection of physical attacks is ensured by the security features of both the IC and the OS, in accordance with the security recommendations contained in the IC guidance documentation [R41][R42][R43].

9.2 Assurance measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [R18].
The implementation is based on a description of the security architecture of the TOE and on a semi-formal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. These documents,

together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

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

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

A secure delivery of the TOE is guaranteed by the application of dedicated procedures. The prevention measures, the checks and all the actions to be performed at the developer's site are described in the secure delivery procedure addressing the family ALC_DEL, while the security measures related to delivery to be applied at the user's site are defined in the pre-personalization guidance. The latter document also addresses the family AGD_PRE.

The necessary information for the document personalization is provided by a dedicated guidance and the information for its usage after delivery to the legitimate holder is provided by the guidance for the operational use. These documents address the AGD_OPE assurance family.

To protect the confidentiality and integrity of the TOE design and implementation, the development and production environment and tools conform to the security policies defined in the documentation dedicated to the development security, which addresses the family ALC_DVS.

The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in dedicated documents addressing the families ALC_LCD and ALC_TAT.

An independent vulnerability analysis, meeting requirements of the family AVA_VAN, is conducted by a third party.

Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the platform (IC) are covered by documents from the IC manufacturer. The security procedures described in such documents have been taken into consideration.

Table 9-2 shows the documentation that provides the necessary information related to the assurance requirements defined in this security target.

Table 9-2 Assurance requirements documentation

Security assurance requirements	Documents
ADV_ARC.1	Security Architecture Description for SOMA-c018 Machine Readable Electronic Document
ADV_FSP.5	Functional Specification for SOMA-c018 Machine Readable Electronic Document
ADV_IMP.1	Source code of SOMA-c018 Machine Readable Electronic Document
ADV_INT.2	TSF Internals Description for SOMA-c018 Machine Readable Electronic Document
ADV_TDS.4	Design Description for SOMA-c018 Machine Readable Electronic Document
AGD_OPE.1	User Guidance for SOMA-c018 Machine Readable Electronic Document
AGD_PRE.1	Initialization Guidance for SOMA-c018 Machine Readable Electronic Document Pre-personalization Guidance for SOMA-c018 Machine Readable Electronic Document Personalization Guidance for SOMA-c018 Machine Readable Electronic Document
ALC_CMC.4, ALC_CMS.5	Configuration management plan Configuration list Evidences of configuration management
ALC_DEL.1	Secure delivery procedure Delivery documentation
ALC_DVS.2	Development security description Development security documentation
ALC_LCD.1	Life cycle definition
ALC_TAT.2	Tools and techniques definition
ATE_COV.2	Test Coverage Analysis for SOMA-c018 Machine Readable Electronic Document
ATE_DPT.3	Test Depth Analysis for SOMA-c018 Machine Readable Electronic Document
ATE_FUN.1	Functional Test Plan for SOMA-c018 Machine Readable Electronic Document Evidences of tests
ATE_IND.2	Documentation related to the independent test
AVA_VAN.5	Documentation related to the independent vulnerability analysis

The assurance measures detailed in this section cover the security assurance requirements described in section 8.3.

10. References

10.1 Acronyms

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

EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EIS	Extended Inspection System
FID	File Identifier
GIS	General Inspection System
GM	Generic Mapping
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
ICCSN	Integrated Circuit Card Serial Number
IM	Integrated Mapping
IS	Inspection System
IT	Information Technology
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PACE	Password Authenticated Connection Establishment
PICC	Proximity Integrated Circuit Chip
PKI	Public Key Infrastructure
PP	Protection Profile
RF	Radio Frequency
RFID	Radio Frequency Identification
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm

SPA	Simple Power Analysis
ST	Security Target
TA	Terminal Authentication
TDES	Triple DES
TOE	Target of Evaluation
TR	Technical Report
TRNG	True Random Number Generator
TSF	TOE Security Functionality
TSP	TOE Security Policy
VIZ	Visual Inspection Zone

10.2 Glossary

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate if the issuing Document Verifier is trusted by the e-Document's chip to produce Terminal Certificates with the correct certificate effective date; see [R14].
Active Authentication (AA)	Security mechanism defined in ICAO Doc 9303 [R23], by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine e-Document, issued by a known state or organization.
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between an e-Document and a terminal as required by [R13], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D, and (iv) Terminal Authentication v.1.
Application Note	Additional information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit Records	Write-only-once non-volatile memory area of the e-Document's chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the e-Document and its data elements on the e-Document's chip were created by the Issuing State or Organization.
Basic Access Control (BAC)	Security mechanism defined by ICAO [R23] by which means the e-Document's chip proves and the inspection

Term	Definition
	system protects their communication by means of secure messaging with the Document BAC Keys.
Basic Inspection System with Basic Access Control Protocol (BIS-BAC)	A technical system being used by an official organization and operated by a governmental organization verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol, and authenticates itself to the e-Document using the Document Basic Access Keys drawn from printed MRZ data for reading the less sensitive data (e-Document details data and biographical data) stored on the e-Document. See [R22] [R23].
Basic Inspection System with PACE Protocol (BIS-PACE)	A technical system being used by an inspecting authority and verifying the e-Document presenter as the e-Document holder (e.g. by comparing the real biometric data (face) of the e-Document presenter with the stored biometric data (DG2) of the e-Document holder). BIS-PACE implements the terminal's part of the PACE protocol, authenticates itself to the e-Document using a shared password (PACE password), and supports Passive Authentication. See [R22] [R23].
Biographical Data	The personalized details of the bearer of the document appearing as text in the Visual Inspection Zone (VIZ) and Machine Readable Zone (MRZ) on the biographical data page of an e-Document [R22].
Biometric Reference Data	Data stored for biometric authentication of the e-Document holder in the e-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 of 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.
Chip Authentication (CA)	Authentication protocol used to verify the genuineness of the e-Document's chip.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.

Term	Definition
Country Signing Certification Authority (CSCA)	An organization enforcing the policy of the e-Document issuer with respect to confirming correctness of user and TSF data stored in the e-Document. The CSCA represents the country specific root of the PKI for the e-Documents 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 [R24]. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [R24]) 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 [R14].
Country Signing Certification Authority Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (PK_{CSCA}) issued by the Country Signing Certification Authority and stored in the inspection system.
Country Verifying Certification Authority (CVCA)	An organization enforcing the privacy policy of the e-Document issuer with respect to protection of user data stored in the e-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 [R14]. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [R24]) 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 [R14].
Current Date	The maximum of the effective dates of valid CVCA, DV, and domestic Inspection System certificates known to the TOE. It is used to validate card verifiable certificates.
CV Certificate	Card Verifiable certificate according to [R14].
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

Term	Definition
	certificate expiration date of the certificate for the old key.
Document Basic Access Keys	Pair of symmetric (two-key) TDES keys used for secure messaging with encryption and message authentication of data transmitted between the e-Document's chip and an inspection system using BAC [R23]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the e-Document; see [R23].
Document Details Data	Data printed on and electronically stored in the e-Document representing the document details like document type, issuing State, document number, date of issue, date of expiry, issuing authority. The document details data are less sensitive data.
Document Security Object (SO_D)	An RFC 3369 Signed Data Structure [R26], signed by the Document Signer (DS). It carries the hash values of the LDS DGs and is stored in the e-Document's chip. It may carry the Document Signer Certificate (C_{DS}) [R22] [R24].
Document Signer (DS)	An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the e-Document for passive authentication. A Document Signer is authorized by the CSCA issuing the Document Signer certificate (C_{DS}); see [R24]. 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 (e.g. of a governmental organization or 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 CVCA to issue certificates for terminals; see [R14]. There can be domestic and foreign DVs. A domestic DV is acting under the policy of the domestic CVCA being run by the e-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 e-Document issuer and a foreign CVCA enforcing the e-Document issuer's privacy policy).
e-Document	An official document of identity issued by a State or Organization, which may be used by the rightful holder.

Term	Definition
e-Document 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 [R22] [R23].
e-Document Holder	The rightful holder of the e-Document for whom the issuing State or Organization personalized the e-Document.
e-Document's Chip	A contact-based/contactless integrated circuit chip complying with ISO/IEC 14443 [R31] [R32] and programmed according to the Logical Data Structure as specified by ICAO [R22].
e-Document's Chip Embedded Software	Software embedded in a e-Document's chip and not being developed by the IC Designer. The e-Document's chip Embedded Software is designed in phase 1 and embedded into the e-Document's chip in Phase 2 of the TOE life cycle.
Eavesdropper	A threat agent with high attack potential reading the communication between the e-Document's chip and the inspection system to gain the data on the e-Document's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [R22].
Extended Access Control (EAC)	Security mechanism identified in BSI TR-03110 [R13] by which means the e-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 the BIS, authorized by the Issuing State or Organization to read the optional biometric reference data and supports the terminal's part of the Extended Access Control authentication mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [R22].

Term	Definition
General Inspection System (GIS)	A Basic Inspection System which implements sensitively the Chip Authentication mechanism.
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 e-Documents.
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.
IC Dedicated Support Software	The 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	The part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery, but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	Unique IC identifier written by the IC Manufacturer onto the chip to control the IC as e-Document material during the IC manufacturing and the delivery process to the Initialization Agent.
IC Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the IC Manufacturer (Phase 2) in Step 3, IC Manufacturing.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person’s document.
Improperly Documented Person	A person who uses, or attempts to use: (a) an expired or invalid document; (b) a counterfeit, forged or altered

Term	Definition
	document; (c) someone else's document; or (d) no document, if required.
Initialization Agent	The agent who initializes the e-Document by writing Initialization Data.
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the IC Manufacturer or by the Initialization Agent (Phase 2). These data are, for instance, used for OS configuration, for traceability, and for IC identification as e-Document's material (IC identification data).
Inspection	The act of a State examining an e-Document presented to it by a user (the e-Document holder) and verifying its authenticity.
Inspection System (IS)	A technical system used by the border control officer of the receiving State or Organization (i) examining an e-Document presented by the user and verifying its authenticity, and (ii) verifying the user as e-Document holder.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The e-Document's chip is an integrated circuit.
Integrity	Ability to confirm the e-Document and its data elements on the e-Document's chip have not been altered from those created by the Issuing State or Organization.
Issuing Organization	Organization authorized to issue an official e-Document (e.g. the United Nations Organization, issuer of the Laissez-passer).
Issuing State	The Country issuing an official e-Document.
Logical Data Structure (LDS)	The collection of groupings of data elements stored in the optional capacity expansion technology [R22]. The capacity expansion technology used is the e-Document's chip.

Term	Definition
Logical e-Document	Data of the e-Document holder stored according to the Logical Data Structure [R22] as specified by ICAO on the contact-based/contactless integrated circuit. It presents contact-based/contactless readable data including (but not limited to): i. personal data of the e-Document holder ii. the digital Machine Readable Zone data (digital MRZ data, EF.DG1), iii. the digitized portraits (EF.DG2), iv. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both, v. the other data according to LDS (EF.DG5 to EF.DG16), vi. 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 various purposes (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 [R22].
Machine Readable Zone (MRZ)	Fixed dimensional area located on the front of the e-Document data page or, in the case of the TD1, the back of the e-Document, containing mandatory and optional data for machine reading using OCR methods [R22]. The MRZ password is a restricted-revealable secret that is derived from the Machine Readable Zone and may be used for both PACE and BAC.
Machine-verifiable Biometrics Feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint, or facial characteristics) stored on an e-Document in a form that can be read and verified by machine [R22].
Metadata of a CV Certificate	Data within the certificate body (except for public key) as described in [R14]. The metadata of a CV certificate comprise the following elements:

Term	Definition
	i. Certificate Profile Identifier, ii. Certificate Authority Reference, iii. Certificate Holder Reference, iv. Certificate Holder Authorisation Template, v. Certificate Effective Date, vi. Certificate Expiration Date.
Optional Biometric Reference Data	Data stored for biometric authentication of the e-Document holder in the e-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 fingerprints and not to use iris images as optional biometric reference data.
PACE Password	A password needed for PACE authentication, e.g. CAN or MRZ.
PACE Terminal (PCT)	A technical system verifying correspondence between the password stored in the e-Document and the related value presented to the terminal by the e-Document presenter. A PCT implements the terminal's part of the PACE protocol, and authenticates itself to the e-Document using a shared password (e.g. CAN or MRZ).
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 data fields with the hash values contained in the Document Security Object; see [R23] [R24].
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [4]. The PACE protocol is a password-authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. a smart card and the terminal connected): i.e. PACE provides a verification whether the communication partners share the same value of a password). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
Personalization	The process by which the personalization data are stored in and unambiguously, inseparably associated with the e-Document. This may also include the optional biometric data collected during the enrolment.

Term	Definition
Personalization Agent	An organization acting on behalf of the e-Document issuer to personalize the e-Document for the e-Document holder by some or all of the following activities: i. establishing the identity of the e-Document holder for the biographic data in the e-Document, ii. enrolling the biometric reference data of the e-Document holder, iii. writing a subset of these data on the physical e-Document (optical personalization) and storing them in the e-Document (electronic personalization) for the e-Document holder as defined in [R22], iv. writing the document details data, v. writing the initial TSF data, vi. signing the Document Security Object defined in [R22] (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 e-Document issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Key	Symmetric cryptographic authentication key used (i) by the Personalization Agent to prove their identity and get access to the logical e-Document, and (ii) by the e-Document's chip to verify the authentication attempt of a terminal as Personalization Agent.
Personalization Data	A set of data incl. (i) individual-related data (biographic and biometric data) of the e-Document holder, (ii) dedicated document details data, and (iii) dedicated initial TSF data (incl. the Document Security Object). Personalization data are gathered and then written into the non-volatile memory of the TOE by the Personalization Agent in the personalization life cycle phase.
Physical e-Document	Electronic document in the form of paper, plastic and chip using secure printing to present data including (but not limited to):

Term	Definition
	i. biographical data, ii. data of the Machine Readable Zone, iii. photographic image, and iv. other data.
Pre-personalization	Process of writing pre-personalization data to the TOE, including the creation of the e-Document application.
Pre-personalization Agent	The agent who performs pre-personalization by writing Pre-personalization Data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Pre-personalization Agent (phase 2) for traceability of non-personalized e-Documents and/or for secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication key pair and the Personalization Agent key.
Presenter	Person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.
Receiving State or Organization	The Country or the Organization to which the e-Document holder is applying for entry or control [R22].
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 [R31] [R32].
Secure Messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R23].
Service Provider	An official organization (inspection authority) providing inspection service which can be used by the e-Document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical e-Document or parts of it via the contact or contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an e-Document and a terminal as required by [R23], namely (i) PACE or BAC and (ii) Passive Authentication with SO_D. The Standard Inspection Procedure can generally be used by BIS-PACE and BIS-BAC.

Term	Definition
Terminal	A terminal is any technical system communicating with the TOE either through the contact-based or contactless interface, verifying correspondence between the password stored in the e-Document and the related value presented to the terminal by the e-Document presenter. A terminal may implement the terminal's part of the PACE protocol, and thus authenticate itself to the e-Document using a shared password (e.g. CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate, and the Country Verifying Certification Authority, which shall be all valid for the Current Date.
TOE Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Initialization Agent (phase 2) in step 5, Initialization.
TOE Tracing Data	Technical information about the current and previous locations of the e-Document gathered by inconspicuously (for the e-Document holder) recognising the e-Document.
TSF Data	Data created by and for the TOE that might affect the operation of the TOE [R16].
User Data	Data created by and for the user that does not affect the operation of the TSF [R16].
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single applicant whose identity is being claimed, to determine whether it matches the applicant's template [R22].
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.

10.3 Technical references

[R1] **ANSSI:** *Rapport de certification ANSSI-CC-2018/12 – S3D350A / S3D300A / S3D264A / S3D232A / S3D200A / S3K350A / S3K300A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated*

[R2] **HID Global:** *Security Target for SOMA-c018 Machine Readable Electronic Document – EAC-PACE-AA, ref. TCAE170049*

[R3] **HID Global:** *Security Target Lite for SOMA-c018 Machine Readable Electronic Document – Basic Access Control, ref. TCLE170096*

[R4] **HID Global:** *Initialization Guidance for SOMA-c018 Machine Readable Electronic Document v1.7, ref. TCAE170050*

[R5] **HID Global:** *Pre-personalization Guidance for SOMA-c018 Machine Readable Electronic Document v1.7, ref. TCAE170051*

[R6] **HID Global:** *Personalization Guidance for SOMA-c018 Machine Readable Electronic Document v1.7, ref. TCAE170052*

[R7] **HID Global:** *Operational User Guidance for SOMA-c018 Machine Readable Electronic Document v1.7, ref. TCAE170053*

[R8] **HID Global:** *Secure Delivery Procedure, ref. TCAE110027*

[R9] **BSI:** *AIS31, Functionality Classes and Evaluation Methodology for Physical Random Number Generators, version 1, September 2001*

[R10] **BSI:** *Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Basic Access Control, Version 1.10, March 2009, ref. BSI-CC-PP-0055*

[R11] **BSI:** *Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, December 2012, ref. BSI-CC-PP-0056-V2-2012*

[R12] **BSI:** *Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, July 2014, ref. BSI-CC-PP-0068-V2-2011-MA-01*

[R13] **BSI:** *Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine*

Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, version 2.20, February 2015

[R14] BSI: *Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, version 2.21, December 2016*

[R15] BSI: *Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.0, June 2012*

[R16] CCMB: *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-001*

[R17] CCMB: *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-002*

[R18] CCMB: *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version 3.1, revision 5, April 2017, ref. CCMB-2017-04-003*

[R19] Certicom Research: *Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, version 2.0, January 2010*

[R20] EMV: *Card Personalization Specification, version 1.0, June 2003*

[R21] Eurosmart: *Security IC Platform Protection Profile with Augmentation Packages, version 1.0, January 2014, ref. BSI-CC-PP-0084-2014*

[R22] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), Seventh Edition, 2015*

[R23] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, Seventh Edition, 2015*

[R24] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs, Seventh Edition, 2015*

[R25] IETF Network Working Group: *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997*

[R26] **IETF Network Working Group:** *Request For Comments 3369, Cryptographic Message Syntax (CMS), August 2002*

[R27] **IETF Network Working Group:** *Request for Comments 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010*

[R28] **ISO/IEC:** *International Standard 7816-2, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts*

[R29] **ISO/IEC:** *International Standard 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*

[R30] **ISO/IEC:** *International Standard 9796-2, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*

[R31] **ISO/IEC:** *International Standard 14443-3, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision*

[R32] **ISO/IEC:** *International Standard 14443-4, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*

[R33] **JIWG:** *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.5, October 2017*

[R34] **NIST:** *FIPS PUB 46-3, Federal Information Processing Standards Publication, Data Encryption Standard (DES), October 1999*

[R35] **NIST:** *FIPS PUB 180-3, Federal Information Processing Standards Publication, Digital Signature Standard, June 2009*

[R36] **NIST:** *FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012*

[R37] **NIST:** *FIPS PUB 186-4, Federal Information Processing Standards Publication, Digital Signature Standard (DSS), July 2013*

[R38] **NIST:** *FIPS PUB 197, Federal Information Processing Standards Publication, Advanced Encryption Standard (AES), November 2001*

[R39] **NIST:** *Special Publication 800-38B, Recommendation for Block Cipher Modes of*

Operation: The CMAC Mode for Authentication, May 2005

[R40] Samsung: *ST (Security Target) Lite – 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 2.1, 25th October 2017*

[R41] Samsung: *S3D350A Series CMOS Microcontroller for Smart Card User's Manual, revision 0.90, April 2017*

[R42] Samsung: *RSA/ECC Library API Manual for S3D350A, S3K250A and S3K170A, version 1.02, October 2017*

[R43] Samsung: *S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note, revision 1.6, 2017-10-12*

Appendix A Integrated circuit Samsung S3D350A (rev2)

The IC on which the TOE is based, constituting the platform for its composite evaluation (cf. [R33]), is the secure microcontroller S3D350A (rev2) with the PKA library (RSA/ECC/SHA) and True Random Number Generation Library (DTRNG), including specific IC Dedicated Software, developed and manufactured by Samsung.

The versions of the two libraries are encoded in the ATR string returned by both the contact and contactless interfaces as follows:

- The version of the PKA library (RSA/ECC/SHA) is encoded in the third to last byte.
- The version of the True Random Number Generation Library (DTRNG) is encoded in the second to last byte.
- In both bytes, the most significant nibble identifies the version major number, and the least significant nibble identifies the version minor number.

In the ATR returned by the TOE identified in section 1.3, the value of the above two bytes shall be 13h 20h, thus identifying version 1.03 of the PKA library (RSA/ECC/SHA) and version 2.0 of the True Random Number Generation Library (DTRNG).
Both of PKA library (RSA/ECC/SHA) version 1.03 and True Random Number Generation Library (DTRNG) version 2.0 are used in the TOE.

This IC has obtained a Common Criteria certification at Evaluation Assurance Level EAL6 augmented by ASE_TSS.2.

The current certification report of chip S3D350A (rev2) is identified in the bibliography (cf. [R1]), and is associated with the following reference code:

ANSSI-CC-2018/12

The current version of the public security target of the chip is identified in the bibliography (cf. [R40]).

END OF DOCUMENT