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

www.hidglobal.com

HIDApp-eDoc suite

Security Target ICAO Application

BAC

Public version

Common Criteria version 3.1 revision 5
Assurance Level EAL4+

Version	1.2
Date	2023-06-07
Reference	TCLE210004
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.

Definitions

The IC Developer is defined as the Platform Developer of the composite product evaluation; the IC Manufacturer is defined as the Platform Manufacturer of the composite product evaluation (see section 2.3).

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 RFC 2119 [R28].

1. Introduction

1.1 ST overview

This document is the sanitized version of the document Security Target for HIDApp-eDoc suite – BAC [R17].

This Security Target (ST) document defines the security objectives and requirements, as well as the scope of the Common Criteria evaluation of HIDApp-eDoc suite.

The Target Of Evaluation (TOE) is the platform NXP JCOP 4 P71 [R41] with application Java Card Applet HID HIDApp-eDoc suite, namely an International Civil Aviation Organization (ICAO) applet compliant with ICAO Doc 9303 8th ed. 2021 – LDS1 [R25] [R26] Eighth Edition, 2021
[R27] and an eIDAS eSign Applet providing qualified signature features (QSCD). The qualified signature features are compliant with the eIDAS Regulation (EU) No 910/2014 [R11] and the according Commission Implementing Decision (EU) 2016/650 [R12], repealing the European Parliament Directive 1999/93/EC [R13]. The eIDAS eSign application is also compliant to the BSI TR-03110-2 [R6] and TR Signature creation and administration for eIDAS token [R1].

The TOE adds security features to a document booklet or card, providing machine-assisted identity confirmation and machine-assisted verification of document security, as well as secure signature creation and data encipherment.

This ST addresses the Basic Access Control (BAC) security mechanism, featured by the ICAO application according to ICAO Doc 9303 8th ed. Part 11 [R26].

The e-Document application also supports the following advanced security methods:

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 8th ed. Part 11 [R26] and Terminal Authentication according to BSI TR-03110 [R6] [R7],
- Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 8th ed. Part 11 [R26] and
- Active Authentication according to ICAO Doc 9303 8th ed. Part 11 [R26]

which are addressed by another ST [R16].

The eIDAS eSign Applet requirements are addressed by still another ST [R18].

1.2 ST reference

Table 1-1 ST reference

Title	Security Target for HIDApp-eDoc suite - ICAO Application - BAC - Public Version
Version	1.2
Authors	Giovanni LICCARDO - Roberta SODANO
Date	2023-06-07
Reference	TCLE210004

1.3 TOE reference

Table 1-2 TOE reference

TOE name	HIDApp-eDoc suite ICAO Application - BAC
TOE version	3_00
TOE developer	HID Global
TOE identifier	HIDApp-eDoc_3_00
TOE identification data	48h 49h 44h 41h 70h 70h 2Dh 65h 44h 6Fh 63h 5Fh 33h 5Fh 30h 30h
Platform security target	JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.11 – 3 January 2023 [R41]
Platform certification report	NSCIB-CC-180212-5MA1 [R47]

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

HIDApp-eDoc_3_00
(ASCII encoding: 48h 49h 44h 41h 70h 70h 2Dh 65h 44h 6Fh 63h 5Fh 33h 5Fh 30h 30h)

where:

- “HIDApp-eDoc” is the TOE name,
- the underscore character is a separator,
- “3” is the TOE major version number and
- “00” is the TOE minor 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 [R19] [R20] [R21] [R22] [R23].

1.4 TOE overview

1.4.1 TOE definition

The TOE is an electronic document representing a smart card programmed according to the Logical Data Structure (LDS) [R25] and providing the Basic Access Control (BAC) according to ICAO Doc 9303 8th edition Part 11 [R26].

The HIDApp-eDoc suite is composed of:

- platform NXP JCOP 4 P71 (see Appendix A), which is composed by the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The software stack can be further split into the following components:
    - Firmware for booting and low level functionality of the Micro Controller (MC FW) like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
    - Software for implementing a Java Card Virtual Machine [R46], a Java Card Runtime Environment [R45] and a Java Card Application Programming Interface [R44] called JCVM, JCRE and JCAPI.
    - Software for implementing content management according to GlobalPlatform [R14] called GlobalPlatform Framework
    - Software for executing native libraries, called Secure Box.
- the applet, composed by
    - an ICAO application LDS1 compliant with ICAO Doc 9303 [R25] [R26] Eighth Edition, 2021
    - **[R27]**[1],
    - the eIDAS eSign application compliant with the eIDAS Regulation (EU) No 910/2014 [R11] and the according Commission Implementing Decision (EU) 2016/650 [R12], repealing the European Parliament Directive 1999/93/EC [R13][2],

---

[1] The EAC, PACE and Active Authentication mechanisms of the ICAO Application are out of the scope of this ST.

[2] The eIDAS eSign Application is out of the scope of this ST.

- the associated guidance documentation [R19] [R20] [R21] [R22] [R23].

On account of its composite nature, the TOE evaluation builds on the evaluation of the underlying platform (chip and operating system).

The TOE supports wired 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 Profile [R4].

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.

The e-Document in context of this protection profile contains

i. visual (eye readable) biographical data and portrait of the holder,
ii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine Readable Zone (MRZ) and
iii. data elements on the e-Document's chip according to LDS for machine reading.

The authentication of the presenter[3] is based on:

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

[3] The person presenting the eDocument to the Inspection System.

The Issuing State or Organization ensures the authenticity of the data of genuine e-Documents, the receiving State or Organization 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 e-Document** as electronic document in the form of paper, 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 e-Document booklet,
  - 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 [R25] 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[4],
  - 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.

Application Note 1 *EF.DG15 is out of the scope of this ST as Active Authentication is not included in the TOE.*

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 e-Document as the book or card and the e-Document's chip are uniquely identified by the Document Number.

The physical e-Document is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the e-Document's chip) and

[4] These biometric reference data are optional according to [R8]. These data are protected by means of Extended Access Control, which is out of scope of this ST.

organizational security measures (e.g. control of materials, personalization procedures). These security measures include the binding of the e-Document's chip to the book or card.

The logical e-Document delivered by the IC Manufacturer to the Initialization Agent is protected by a SCP03 mechanism. After completion, the authentication keys are changed. The logical e-Document delivered by the Initialization Agent to the Personalization Agent is protected by a SCP03 mechanism until completion of the Personalization process. After completion, all the privileges are disabled with the exception of CARD_LOCKED and TERMINATED, see section 6.6 of [R14].

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 the logical e-Document and
- the Data Encryption of sensitive biometrics as an optional security measure in the ICAO Doc 9303 [R26].

The Passive Authentication and the Data Encryption are 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 Basic Access Control Mechanism.

<u>This security target does not address Active Authentication and Extended Access Control as optional security mechanisms.</u>

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system:

i. reads optically the e-Document,
ii. authenticates itself as inspection system by means of Document Basic Access Keys.

After successful authentication of the inspection system, the e-Document chip provides read access to the logical e-Document by means of private communication (secure messaging) with this inspection system [R26], section 9.8.

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 applet. Note, the substrate holding the chip as well as the antenna and the booklet or plastic card (holding the printed MRZ) 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 Platform by the IC Developer,

   Step 2: the development of the Applet by the Applet Developer;

2. Phase 2: Manufacturing comprises:

   Step 3: the fabrication of the Platform by the IC Manufacturer,

   Step 4: the loading of the Applet by the IC Manufacturer,

   Step 5: the embedding of the chip in a substrate with an antenna (the antenna may be omitted if the IC contacts are exposed),

   Step 6: the Applet initialization;

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.

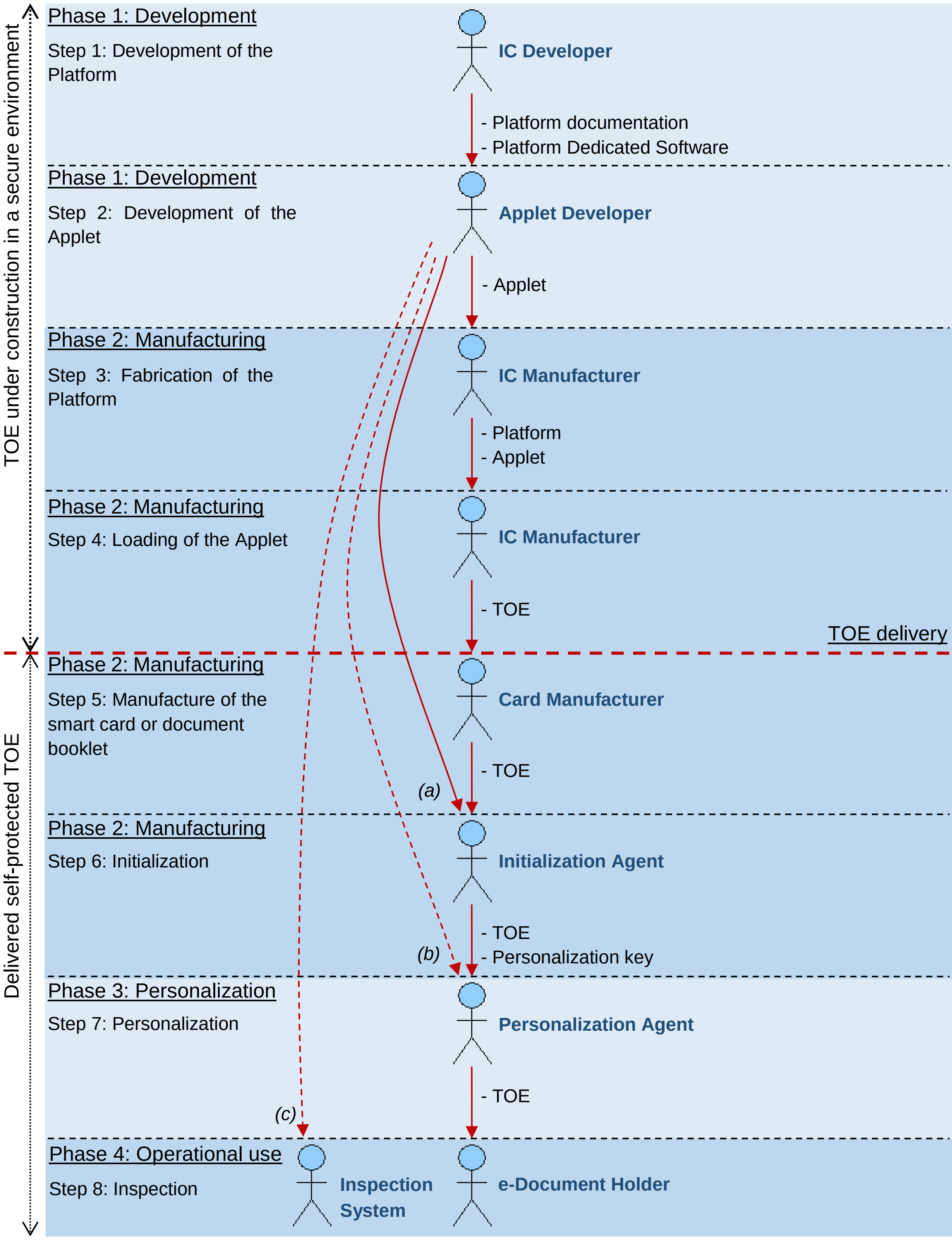
Application Note 2 *The entire Development phase, as well as Step 3 "*the fabrication of the Platform*" and Step 4 "Loading the Applet" of the Manufacturing phase are the only phases covered by assurance under ALC, as during these phases the TOE is under construction in a protected environment.*

Figure 1-1 represents the life cycle of the ICAO application. 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 dashed 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 key • Initialization guidance
(b)	• Personalization guidance
(c)	• Operational user guidance

Figure 1-1 Life cycle of the TOE ICAO application



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
1	IC Developer	NXP
1	Applet Developer	HID Global
2	IC Manufacturer	NXP
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.
2	Initialization Agent	The agent who is acting on behalf of the issuing state or organization to load the personalization key.
2	*Manufacturer*	Role that collectively identifies all the agents acting in phase 2, namely: • the IC Manufacturer, • the Card Manufacturer, • the Initialization Agent.
3	Personalization Agent	The agent who is acting on behalf of the issuing state or organization to personalize the e-Document for the holder.
4	e-Document Holder	The rightful owner of the e-Document.
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.

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
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 Platform

The **IC Developer** develops the JCOP 4 P71 Platform, the platform dedicated software and the guidance documentation associated with these TOE components.

Finally, the following items are securely delivered to the **Applet Developer**:

- the Platform documentation,
- the Platform dedicated software,

Step 2: Development of the Applet

The **Applet Developer** uses the guidance documentation for the Platform and for relevant parts of the Platform Dedicated Software and develops the applets, consisting of the ICAO application and the eIDAS eSign application, as well as the guidance documentation associated with these TOE components.

Furthermore, the **Applet Developer** generates the initialization key.

Finally:

- the Applet is securely delivered to the **IC Manufacturer**;
- the initialization key are securely delivered to the **Initialization 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: Fabrication of the platform

The **IC Manufacturer** produces the JCOP 4 P71 Platform.

Step 4: Loading of the Applet

The **IC Manufacturer** loads the Applet received from the Applet Developer 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 3 *The point of delivery of the TOE coincides with the completion of step 4, 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 5: 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 6: Initialization

The **Initialization Agent** use the initialization key to mutual authentication with the TOE to instantiate ICAO applet and writes the Personalization Key.

Finally, the TOE is securely delivered to the **Personalization Agent**, along with the personalization key if it was delivered to the **Initialization Agent** rather than directly to the **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 **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 [R25] Eighth Edition, 2021
[R27] finalizes the personalization of the genuine e-Document for the document holder.

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. [R8], section 92) comprise (but are not limited to) the initialization 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 [R25] and Eighth* Edition, 2021
Application Note 6 **[R27]**. *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 7 *This ST considers phase 1 and parts of phase 2 (i.e. step 1 to step 4) as part of the evaluation, and therefore defines the TOE delivery according to CC after step 4. 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.*

1.6 TOE description

1.6.1 Physical scope of the TOE

The HIDApp-eDoc suite is comprised of the following parts:

- The platform NXP JCOP 4 P71 (see Appendix A), which is composed by the Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. The software stack can be further split into the following components:
    - Firmware for booting and low level functionality of the Micro Controller (MC FW) like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
    - Software for implementing a Java Card Virtual Machine [R46], a Java Card Runtime Environment [R45] and a Java Card Application Programming Interface [R44] called JCVM, JCRE and JCAPI.
    - Software for implementing content management according to GlobalPlatform [R14] called GlobalPlatform Framework
    - Software for executing native libraries, called Secure Box.
- the applet, composed by

- ICAO Application compliant with ICAO Doc 9303 [R25][R26]Eighth Edition, 2021
- [R27][5],
- the eIDAS eSign application compliant with the eIDAS Regulation (EU) No 910/2014 [R11] and the according Commission Implementing Decision (EU) 2016/650 [R12], repealing the European Parliament Directive 1999/93/EC [R13][6],

- guidance documentation about the initialization of the TOE, the preparation and use of the ICAO application and eIDAS eSign application, composed by:
  - the Initialization Guidance [R19]
  - the Personalization Guidance [R20] - ICAO application,
  - the Operational User Guidance [R22] - ICAO application.
  - the Personalization Guidance [R21] - eIDAS eSign application,
  - the Operational User Guidance [R23] - eIDAS eSign application,

Table 1-5 identifies, for each guidance document, the actors involved in TOE life cycle who are the intended recipients of that document.

Table 1-6 described the format and delivery method of each TOE components:

Table 1-6 TOE component delivery

Type	TOE component	Format	Delivery method
Platform	NXP JCOP 4 P71	Smart Card	Secure courier
Applet	HIDApp-eDoc suite	CAP file	Secure IC Manufacturer's Web application
Document	Preparative and operational guidance	pdf/docx	Encrypted email message

The delivery procedure for the TOE is described in detail [R24].

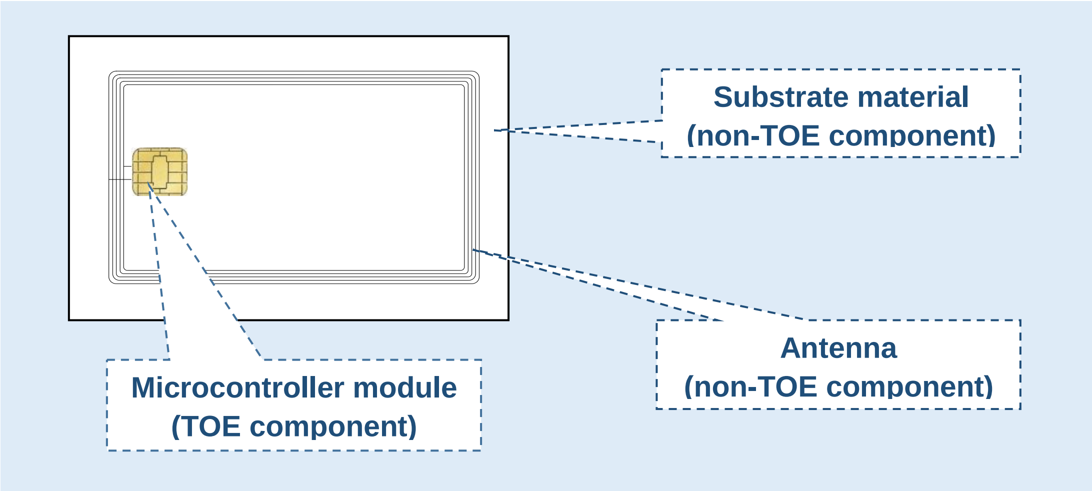
1.6.2 Other non-TOE physical components

[5] The EAC, PACE and Active Authentication mechanisms of the ICAO Application are out of the scope of this ST.

[6] The eIDAS eSign Application is out of the scope of this ST.

The antenna and the substrate are not part of the TOE.
Figure 1-2 shows the smart card 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 HIDApp-eDoc 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 6, Initialization, of phase 2, the Initialization Agent must prove his/her identity by means of an authentication mechanism based on SCP03 with AES 256-bit key.
- In phase 3, Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on SCP03 with AES 256-bit key.
- 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 BAC mechanism compliant to ICAO Doc 9303-11 [R26].

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 [R31].

The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism defined in [R26]. BAC and Passive Authentication mechanisms are described in more detail in the following subsections.

1.6.3.1 Passive Authentication

Passive Authentication consists of the following steps (cf. [R26]):

1. The inspection system reads the Document Security Object (SO_D), which contains the Document Signer Certificate (C_{DS}, cf. [R25]), 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 [R25].
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 Basic Access Control

Basic Access Control provides mutual authentication and session key establishment by means of a three-step challenge-response protocol according to [R33], Key Establishment Mechanism 6, using Triple DES [R37] as block cipher. A cryptographic checksum according to [R32], MAC Algorithm 3, is calculated over and appended to the ciphertexts. The modes of operation described in [R26] are used. Exchanged nonces must be 8 bytes long, exchanged keying material must be 16 bytes long.

2. Conformance claims

2.1 Common Criteria conformance claim

This security target claims conformance to:

- Common Criteria version 3.1 revision 5 [R8] [R9] [R10], as follows:
  - Part 2 (security functional requirements) extended,
  - Part 3 (security assurance requirements) conformant.

The applet runs on the platform NXP JCOP 4 P71. This platform is certified against Common Criteria at the assurance level EAL6+ (cf. Appendix A).

2.2 Package conformance claim

This security target claims conformance to:

- EAL4 assurance package augmented by ALC_DVS.2, as defined in CC part 3 [R10].

2.2.1 Protection Profile conformance claim

This security target claims strict conformance to:

- BSI-CC-PP-0055, Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Basic Access Control, version 1.10, March 2009 [R4].

2.3 Protection Profile conformance rationale

This security target claims strict conformance to the BAC PP [R4]. The parts of the TOE listed in that Protection Profile correspond to the ones listed in section 1.4.1 of this ST.

This ST adopts as a reference the ICAO Doc 9303 Eighth Edition 2021. Due to this update, any references to the ICAO Doc 9303 2006 specification in the BAC PP have been replaced with references to the ICAO Doc 9303 2021.

The TOE is a composed TOE, based on NXP JCOP 4 P71 that is a composed TOE itself. For this reason, the acronym "IC" used in the PPs and referred in this Security Target stands for "platform".

Being the TOE a general purpose electronic document, all references in the PP to the use of the TOE for travel have been removed in this ST. For the same reason, with respect to the PP, 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 blue.

With respect to the PP, the role “MRTD Manufacturer” has been split into the roles Card Manufacturer and Initialization Agent, acting in Phase 2 “Manufacturing” respectively in Step 5, Card Manufacturing and Step 6, Initialization. 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 and the Initialization 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 4 “Loading of the Applet” of Phase 2, as a chip, in accordance with Application Note 5 of the PP [R4]. At TOE delivery, there is no user data or machine-readable data available.

Concerning Initialization Data, this ST distinguishes between IC Initialization Data written in Step 4 by the IC Manufacturer and TOE Initialization Data written in Step 6 by the Initialization Agent.
The TOE provides a contact interface according to ISO/IEC 7816-2 [R30]; therefore, in addition to the contactless interface referred in the PP, this ST makes also references to the contact interface.

Table 2-1 describes the changes and additions made to the security problem definition and to the security objectives with respect to the PP [R4].

Table 2-1 Modified elements in the security problem definition and security objectives

Element	Definition	Operation
T.Chip_ID	Identification of e-Document’s chip	The definition has been extended to take into account the presence of a contact interface.
T.Skimming	Skimming the logical e-Document	The definition has been extended to take into account the presence of a contact interface.
P.Manufact	Manufacturing of the e-Document’s chip	Modified to distinguish between IC Initialization Data and TOE Initialization Data.

OT.AC_Init	Access control for Initialization of logical e-Document	Added to take into account access control in Step 6, Initialization.
OT.AC_Pers	Access Control for Personalization of logical e-Document.	The definition has been modified in a more restrictive way as data addition is not allowed at all after personalization. In the SFRs rationale, OT.AC_Pers is not mapped to FIA_UAU.6 as the BAC mechanism is not used in Personalization.
OT.Identification	Identification and Authentication of the TOE	Modified in a more restrictive way as access to TOE identification data in Phase 4 is restricted to a BAC authenticated inspection system only (the Personalization Agent cannot access identification data after personalization). Moreover, the objective specifies that the Initialization Data are split into IC Initialization Data and TOE Initialization Data, that the IC Initialization Data include the Initialization Key, and that the TOE Initialization Data include the Personalization Keys.
OE.Initialization	Initialization of logical e-Document	Added to take into account responsibilities in Step 6, Initialization.

The security functional requirements described in section 6 of this ST correspond to the ones in section 5 of the PP [R4].
Table 2-2 shows assignment changes or refinements/iterations/additions with respect to the PP security functional requirements for the TOE. These changes do not lower the TOE security and, in some cases, changed requirements are more restrictive than the ones from the PP.

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

Security functional requirement	Operation
FCS_CKM.1/SCP	**Iteration** Iteration that specifies the generation of the session keys for the Initialization Agent and for the Personalization Agent.
FCS_CKM.1/BAC	**Iteration** Due to the addition of FCS_CKM.1/SCP, an iteration label “BAC” has been added to this SFR to distinguish the generation of BAC session keys.

Security functional requirement	Operation
FCS_COP.1/ENC	**Change** Having FIPS 46-3 been withdrawn, NIST SP 800-67 and SP 800-38A have been referenced instead. See Application Note 25.
FIA_UAU.5.2	**Refinement** A technical reference to the symmetric authentication mechanism with Personalization keys has been added. Moreover, the addition has been performed of the Initialization Agent and the Pre-personalization Agent among the users allowed to authenticate to the e-Document.
FIA_AFL.1/Init FIA_AFL.1/Pers FIA_AFL.1/BAC	**Iteration** Iterations have been added to distinguish between authentication failure handling throughout the TOE life cycle.
FDP_ACC.1	**Refinement** This SFR has been refined with respect to the PP to indicate that the objects of the access control policy also include the initialization data.
FDP_ACF.1	**Refinement** This SFR has been refined with respect to the PP to indicate that the access control is also extended to the initialization data involving the Initialization Agent role.
FMT_MTD.1/KEY_READ/Init FMT_MTD.1/KEY_READ/BAC	**Iteration** Iterations have been added to indicate that read access restriction applies also to the Initialization key. The iteration label “BAC” has been added to the original SFR from the PP to distinguish it from the other iterations.

3. Security problem definition

3.1 Introduction

3.1.1 Assets

The assets to be protected by the TOE include the User Data on the e-Document's chip.

Logical e-Document sensitive User Data

The logical e-Document data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [R25]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the e-Document holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The Active Authentication public key (EF.DG.15) is used by the inspection system for the Active Authentication (note that both Chip Authentication and Active Authentication are out of the scope of this ST). The EF.SOD is used by the inspection system for Passive Authentication of the logical e-Document.

Due to interoperability reasons (cf. ICAO Doc 9303 [R26]), the TOE described in this security target specifies only the BAC mechanism with resistance against enhanced-basic attack potential granting access to

- Logical e-Document standard User Data (i.e. Personal Data) of the e-Document holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common Data in EF.COM.

The TOE prevents read access to sensitive User Data

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

A sensitive asset is the following more general one.

Authenticity of the e-Document's chip

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

3.1.2 Subjects

This security target considers the following subjects:

- **Manufacturer**: The generic term for the IC Manufacturer, the Card Manufacturer and the Initialization Agent. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. This ST also refers to the subjects acting in each of the four steps of the manufacturing phase, namely:
  - the IC Manufacturer in Steps 3 and 4,
  - the Card Manufacturer in Step 5, and
  - the Initialization Agent in Step 6, and

  The subject Manufacturer collectively identifies the above subjects (see also section 2.3).

- **Personalization Agent**: The agent who is acting on behalf of the issuing State or Organization to personalize the e-Document for the holder by some or all the following activities:
  (i) establishing the identity of the holder for the biographic data in the e-Document,
  (ii) enrolling the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s),
  (iii) writing these data on the physical and logical e-Document for the holder as defined for global, international, and national interoperability,
  (iv) writing the initial TSF data, and
  (v) signing the Document Security Object (SO_D) as defined in the ICAO Doc 9303 [R25] Eighth Edition, 2021
  (vi) **[R27]**.

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

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

The **Basic Inspection System** (BIS):

(i) contains a terminal for the contact or contactless communication with the e-Document's chip,

(ii) implements the terminals part of the BAC Mechanism, and

(iii) gets the authorization to read the logical e-Document under the BAC by optically reading the printed data in the MRZ or other parts of the e-Document book or card providing this information.

The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.

The **Extended Inspection System** (EIS) in addition to the General Inspection System

(i) implements the Terminal Authentication protocol, and

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

The security attributes of the EIS are defined by the Inspection System Certificates.

Application Note 8 *This Security Target does not distinguish between the BIS, GIS and EIS because the Chip Authentication and the Extended Access Control mechanisms are out of the scope of this ST.*

- **e-Document Holder**: The rightful holder of the e-Document for whom the issuing State or Organization personalized the e-Document.
- **Presenter**: A person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.
- **Attacker**: A threat agent trying:

  (i) To identify and to trace the movement of the e-Document's chip remotely (i.e. without knowing or optically reading the printed MRZ data),

  (ii) To read or manipulate the logical e-Document without authorization, or

  (iii) To forge a genuine e-Document

Application Note 9 *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.*

3.2 Assumptions

The assumptions describe the security aspects concerning the TOE.

3.2.1 A.e-Document_Manufact

e-Document manufacturing on steps 5 to 7

It is assumed that appropriate functionality testing of the e-Document is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the e-Document and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft of unauthorized use).

3.2.2 A.e-Document_Delivery

e-Document delivery during steps 5 to 7

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

3.2.3 A.Pers_Agent

Personalization of the e-Document's chip

The Personalization Agent ensures the correctness of:

(i) the logical e-Document with respect to the e-Document holder,

(ii) the Document BAC Keys,

(iii) the Chip Authentication Public Key (EF.DG14) if stored on the e-Document's chip, and

(iv) the Document Signer Public Key Certificate (if stored on the e-Document's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

3.2.4 A.Insp_Sys

Inspection Systems for global interoperability

The Inspection System is used by a 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 presenter as e-Document holder.

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 the Basic Access Control [R26].

The Basic Inspection System reads the logical e-Document being under Basic Access Control and performs the Passive Authentication to verify the logical e-Document.

Application Note 10 *According to [R26], the support of Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems, therefore the BAC is mandatory within this ST.*

3.2.5 A.BAC-Keys

Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [R26], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced-basic attack potential.

Application Note 11 *When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.*

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.Chip_ID

Identification of e-Document's chip

Adverse action: An attacker trying to trace the movement of the e-Document by identifying the e-Document's chip directly by establishing a communication through the contact interface or remotely by establishing or listening to communications through the contactless communication interface.

Threat agent: having enhanced-basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: anonymity of user

3.3.2 T.Skimming

Skimming the logical e-Document

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical e-Document or parts of it via the contact or contactless communication channels of the TOE.

Threat agent: having enhanced-basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data

3.3.3 T.Eavesdropping

Eavesdropping to the communication between TOE and inspection system

Adverse action: An attacker is listening communication between the e-Document's chip and an inspection system to gain the logical e-Document or parts of it. The inspection system uses the MRZ data printed on the e-Document data page but the attacker does not know these data in advance.

Threat agent: having enhanced-basic attack potential, not knowing the optically readable MRZ data printed on the e-Document data page in advance.

Asset: confidentiality of logical e-Document data

3.3.4 T.Forgery

Forgery of data on e-Document's chip

Adverse action: An attacker alters fraudulently the complete stored logical e-Document or any part of it including its security related data in order to deceive on an inspection system by means of the changed e-Document holder's identity or biometric reference data. This threat comprises several attack scenarios of e-Document forgery. The attacker may alter the biographical data on the biographical data page or section of the e-Document book or card, in the printed MRZ and in the digital MRZ to claim another identity of the presenter. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical e-Documents to create a new forged e-Document, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical e-Document of a holder into another e-Document's chip leaving their digital MRZ unchanged to claim the identity of the holder this e-Document. The attacker may also copy the complete unchanged logical e-Document to another chip.

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

Asset: authenticity of logical e-Document data

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 the phase "Operational Use" in order:

(i) to manipulate User Data,

(ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE, or

(iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to e-Document holder.

Threat agent: having enhanced-basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

3.3.6 T.Information_Leakage

Information Leakage from e-Document's chip

Adverse action: An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. 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 the Differential

Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover, the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

Threat agent: having enhanced-basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality logical e-Document and TSF data

3.3.7 T.Phys-Tamper

Physical Tampering

Adverse action: An attacker may perform physical probing of the e-Document's chip in order:

(i) to disclose TSF Data, or

(ii) to disclose/reconstruct the e-Document's chip Embedded Software.

An attacker may physically modify the e-Document's chip in order to:

(i) modify security features or functions of the e-Document's chip,

(ii) modify security functions of the e-Document's chip Embedded Software,

(iii) modify User Data, or

(iv) modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the e-Document's chip) 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 direct interaction with the e-Document's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and 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.

Threat agent: having enhanced-basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

3.3.8 T.Malfunction

Malfunction due to Environmental Stress

Adverse action: An attacker may cause a malfunction of TSF or of the e-Document's chip Embedded Software by applying environmental stress in order to:

(i) deactivate or modify security features or functions of the TOE, or

(ii) circumvent or deactivate or modify security functions of the e-Document's chip Embedded Software.

This may be achieved e.g. by operating the e-Document's chip outside the normal operating conditions, exploiting errors in the e-Document's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having enhanced-basic attack potential, being in possession of a legitimate e-Document

Asset: confidentiality and authenticity of logical e-Document and TSF data, correctness of TSF

3.4 Organizational Security Policies

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2 [R8]).

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 writes the keys for the authentication of the Personalization Agent.
The Initialization Agent is authorized by the Issuing State or Organization only.

3.4.2 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-Document for the holder is performed by an agent authorized by the Issuing State or Organization only.

3.4.3 P.Personal_Data

Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the e-Document's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4)[7] and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the e-Document's chip are personal data of the e-Document holder. These data groups are intended to be used only with agreement of the e-Document holder by inspection systems to which the e-Document is presented. The e-Document's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [R26].

Application Note 12 *The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [R26]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.*

[7] Note that EF.DG3 and EF.DG4 are only readable after a successful EAC authentication, not being covered by this security target.

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 TOE Initialization data, which include the Personalization key, can be written in Step 6 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_Pers

Access Control for Personalization of logical e-Document

The TOE must ensure that the logical e-Document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [R25], and the TSF data can be written by an authorized Personalization Agent only. The logical e-Document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization.

Application Note 13 *The OT.AC_Pers implies that*

(1) *The data of the LDS groups written during personalization for the e-Document holder (at least EF.DG1 and EF.DG2) cannot be changed by write access after personalization,*

(2) *The Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the “Operational Use” phase is not provided.*

4.1.3 OT.Data_Int

Integrity of personal data

The TOE must ensure the integrity of the logical e-Document stored on the e-Document's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical e-Document data.

4.1.4 OT.Data_Conf

Confidentiality of personal data

The TOE must ensure the confidentiality of the logical e-Document data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical e-Document data during their transmission to the Basic Inspection System.

Application Note 14 *The holder grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the e-Document. The e-Document's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore, the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [R26] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus, the read access must be prevented even in case of a successful BAC Authentication.*

4.1.5 OT.Identification

Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and other Initialization data, as well as Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization 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 Personalization key(s). In phase 4 “Operational Use”, when using the ICAO application, the TOE shall identify itself only to a successfully authenticated Basic Inspection System.

Application Note 15 *The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or secure shipment of the TOE from Phase 2 “Manufacturing” to Phase 3 “Personalization of the e-Document”. OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 “Operational Use”, the TOE is identified by the Document Number as part of the printed and digital MRZ. OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number, ICCSN) or e-Document identifier through the contact or contactless interfaces before successful authentication as Basic Inspection System*.

The following TOE security objectives address the protection provided by the e-Document’s chip independent on the TOE environment.

4.1.6 OT.Prot_Abuse-Func

Protection against Abuse of Functionality

After delivery of the TOE to the e-Document Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to:

(i) disclose critical User Data,

(ii) manipulate critical User Data of the IC Embedded Software,

(iii) manipulate Soft-coded IC Embedded Software, or

(iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

4.1.7 OT.Prot_Inf_Leak

Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the e-Document's chip

- 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, and
- by forcing a malfunction of the TOE, and/or
- by a physical manipulation of the TOE.

Application Note 16 *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.*

4.1.8 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 chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of

- measuring through galvanic contacts which is direct physical probing on the chips 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 functions.

4.1.9 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 has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application Note 17 *A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.*

4.2 Security objectives for the operational environment

Issuing State or Organization

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

4.2.1 OE.e-Document_Manufact

Protection of the e-Document Manufacturing

Appropriate functionality testing of the TOE shall be used in step 5 to 7.
During all manufacturing and test operations, security procedures shall be used through steps 5, 6 and 7 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

4.2.2 OE.e-Document_Delivery

Protection of the e-Document delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),

- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

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 TSF data for the e-Document,

(ii) 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.Personalization

Personalization of logical e-Document

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

(i) establish the correct identity of the holder and create biographical data for the e-Document,

(ii) enrol the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), and

(iii) personalize the e-Document for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

4.2.5 OE.Pass_Auth_Sign

Authentication of logical e-Document by Signature

The issuing State or Organization must:

(i) generate a cryptographic secure Country Signing CA Key Pair,

(ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and

(iii) distribute the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must:

(i) generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys,

(ii) sign Document Security Objects of genuine e-Document in a secure operational environment only, and

(iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object relates to all data in the data groups EF.DG1 to EF.DG16 if stored in the LDS according to [R25] and Eighth Edition, 2021 **[R27]**.

4.2.6 OE.BAC-Keys

Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' [6] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced-basic attack potential.

Receiving State or Organization

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

4.2.7 OE.Exam_e-Document

Examination of the e-Document book or card

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 e-Document. The Basic Inspection System for global interoperability

(i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

(ii) implements the terminal part of the Basic Access Control [R26].

4.2.8 OE.Passive_Auth_Verif

Verification by Passive Authentication

The control officer of the receiving State or Organization uses the inspection system to verify the presenter as e-Document holder. The inspection systems must have successfully verified the signature of the Document Security Object and the integrity of the data elements of the logical e-Document before they are used. The Receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

4.2.9 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 receiving State or Organization examining the logical e-Document being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security objective rationale

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

Table 4-1 Security objective rationale

	OT.AC_Init	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.e-Document_Manufact	OE.e-Document_Delivery	OE.Initialization	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_e-Document	OE.Passive_Auth_Verif	OE.Prot_Logical_e-Document
T.Chip-ID					X										X			
T.Skimming				X											X			
T.Eavesdropping				X														
T.Forgery	X	X	X					X				X	X	X		X	X	
T.Abuse-Func						X						X	X					
T.Information_Leakage							X											
T.Phys-Tamper								X										
T.Malfunction									X									
P.Manufact	X				X													
P.Personalization		X			X								X					
P.Personal_Data			X	X														
A.e-Document_Manufact										X		X						
A.e-Document_Delivery											X							
A.Pers_Agent													X					
A.Insp_Sys																X		X
A.BAC_Keys															X			

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 TOE Initialization Data as being fulfilled by ***OT.Identification***.

Note that:

- 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 to the Initialization Agent.

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 that:

- the Initialization 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.Personal_Data** "Personal data protection policy" requires the TOE

(i) to support the protection of the confidentiality of the logical e-Document by means of the Basic Access Control, and

(ii) enforce the access control for reading as decided by the issuing State or Organization.

This policy is implemented by the security objectives ***OT.Data_Int*** "Integrity of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective ***OT.Data_Conf*** "Confidentiality of personal data" describes the protection of the confidentiality.

The threat **T.Chip_ID** "Identification of e-Document's chip" addresses the trace of the e-Document movement by identifying remotely the e-Document's chip through the contact communication interface, or remotely through the contactless communication interface. This threat is countered as described by the security objective ***OT.Identification*** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment ***OE.BAC-Keys***.

The threats **T.Skimming** "Skimming digital MRZ data or the digital portrait" and **T.Eavesdropping** "Eavesdropping to the communication between TOE and inspection system" address the reading of the logical e-Document through the contact or contactless interfaces or listening the communication between the e-Document's chip and a terminal. This threat is countered by the security objective ***OT.Data_Conf*** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment ***OE.BAC-Keys***.

The threat **T.Forgery** "Forgery of data on e-Document's chip" addresses the fraudulent alteration of the complete stored logical e-Document or any part of it. The security objectives ***OT.AC_Init***, Initialization of logical e-Document and ***OT.AC_Pers***, Access Control for Personalization of logical e-Document, require the TOE to limit the write access for the logical e-Document to the trustworthy Initialization Agent (cf. ***OE.Initialization***) and Personalization Agent (cf. ***OE.Personalization***). The TOE will protect the integrity of the stored logical e-Document according the security objective ***OT.Data_Int*** "Integrity of personal data" and ***OT.Prot_Phys-Tamper*** "Protection against Physical Tampering". The examination of the presented e-Document book or card according to ***OE.Exam_e-Document*** "Examination of the e-Document book or card" shall ensure that the book or card does not contain a sensitive chip which may present the complete unchanged logical e-Document. The TOE environment will detect partly forged logical e-Document data by means of digital signature which will be created according to ***OE.Pass_Auth_Sign*** "Authentication of logical e-Document by Signature" and verified by the inspection system according to ***OE.Passive_Auth_Verif*** "Verification by Passive Authentication".

The threat **T.Abuse-Func** "Abuse of Functionality" addresses attacks using the e-Document's chip as production material for the e-Document and misuse of the functions for personalization in the operational state after delivery to e-Document holder to disclose or to manipulate the logical e-Document. This threat is countered by ***OT.Prot_Abuse-Func*** "Protection against Abuse of Functionality". Additionally, this objective is supported by the security objectives for the TOE environment ***OE.Initialization***, Initialization of logical e-Document and ***OE.Personalization***, Personalization of logical e-Document, which ensure that the TOE security functions for initialization and personalization are disabled and the security functions for the operational state after delivery to the e-Document holder are enabled according to the intended use of the TOE.

The threats **T.Information_Leakage** "Information Leakage from e-Document's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives ***OT.Prot_Inf_Leak*** "Protection against Information Leakage", ***OT.Prot_Phys-Tamper*** "Protection against Physical Tampering" and ***OT.Prot_Malfunction*** "Protection against Malfunctions".

The assumption **A.e-Document_Manufact** "e-Document manufacturing on step 5 to 7" is covered by the security objectives for the TOE environment ***OE.Initialization***, Initialization of the logical e-Document and ***OE.e-Document_Manufact***, Protection of the e-Document Manufacturing, that requires to use security procedures during all manufacturing steps.

The assumption **A.e-Document_Delivery** "e-Document delivery during step 5 to 7" is covered by the security objective for the TOE environment ***OE.e-Document_Delivery*** "Protection of the e-Document delivery" that requires to use security procedures during delivery steps of the e-Document.

The assumption **A.Pers_Agent** "Personalization of the e-Document's chip" is covered by the security objective for the TOE environment ***OE.Personalization*** "Personalization of logical e-Document" including the enrolment, the protection with digital signature and the storage of the e-Document holder personal data.

The examination of the e-Document book or card addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment ***OE.Exam_e-Document*** "Examination of the e-Document book or card". The security objective for the TOE environment ***OE.Prot_Logical_e-Document*** "Protection of data from the logical e-Document" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical e-Document data during the transmission and the internal handling.

The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment ***OE.BAC-Keys*** "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

5. Extended components definition

This security target uses components defined as extensions to CC part 2 [R9]. All of these components are defined in the PP [R4].

5.1 Definition of family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined in the PP [R4]. 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 in the following table.

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 Audit data storage — 1
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 define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in the PP [R4]. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND 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 in the following table.

Table 5-2 Family FCS_RND

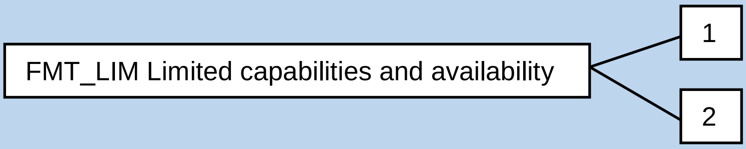
FCS_RND Generation of random numbers	
Family behaviour:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component levelling:	FCS_RND Generation of random numbers — 1
FCS_RND.1	Generation of random numbers requires 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 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 the 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 5-3 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 require 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.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family 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 the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

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*].

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

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 18 *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 policy.

5.4 Definition of family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the PP [R4] to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data 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 which are not directly addressed by any other component of CC part 2 [R9].

The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Table 5-4 Family FPT_EMSEC

FPT_EMSEC TOE emanation	
Family behaviour:	This family defines requirements to mitigate intelligible emanations.
Component levelling:	FPT_EMSEC TOE emanation — 1
FPT_EMSEC.1	TOE emanation has two constituents: • FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. • FPT_EMSEC.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_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components
Dependencies:	No dependencies.
FPT_EMSEC.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_EMSEC.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 [R8] 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.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System", 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 in section 0. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [R9].

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[8] with the capability to store the IC Identification Data[9] in the audit records.

Application Note 19 *The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC Manufacturer and the Initialization Agent in the Manufacturer role write the Initialization Data as TSF Data of the TOE. The audit records are write-only-once data of the e-Document's chip (see FMT_MTD.1/INI_DIS).*

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/BAC

Cryptographic key generation – Generation of Document Basic Access 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/BAC:

[8] [assignment: *authorised user*]
[9] [assignment: *list of audit information*]

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: Document Basic Access Key Derivation Algorithm[10] and specified cryptographic key sizes 112 bit[11], that meet the following: [R26], appendix D.1[12].

Application Note 20 *The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [R26], section 4.3, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [R26], section 9.7.4. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.*

6.2.2 FCS_CKM.1/SCP

Cryptographic key generation – Generation of session Keys for Personalization 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/SCP:

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Secure Channel Protocol '03'** [13] and specified cryptographic key sizes **256 bit**[14] that meet the following: **[R15], section 6.2**[15].

Application Note 21 *The TSF allows to generate the session keys for the initialization and personalization processes by the algorithm described in section 6.2 of the Secure Channel Protocol '03' specification [R15], using the keys stored on the platform (the Initialization key in phase 2 and the Personalization keys in phase 3) and a sequence counter*

---

[10] [assignment: *cryptographic key generation algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]
[13] [assignment: *cryptographic key generation algorithm*]
[14] [assignment: *cryptographic key sizes*
[15] [assignment: *list of standards*]

provided by the Platform to the initialization terminal or to the personalization terminal in response to an INITIALIZE UPDATE command.

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

6.2.3 FCS_CKM.4

Cryptographic key destruction – e-Document

Hierarchical to: No other components.

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

FCS_CKM.4.1:

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: **physical deletion by overwriting the memory data with zeros**[16] that meets the following: **none**[17].

Application Note 22 *The TOE shall destroy the Initialization Key, as well as the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.*

Application Note 23 *Cryptographic keys are destroyed by calling a dedicated interface of the Platform Crypto Library.*

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.

---

[16] [assignment: *cryptographic key destruction method*]
[17] [assignment: *list of standards*]

6.2.4 FCS_COP.1/SHA

Cryptographic operation – Hash for Key Derivation

Hierarchical to: No other components.

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

FCS_COP.1.1/SHA:

The TSF shall perform hashing[18] in accordance with a specified cryptographic algorithm **SHA-1**[19] and cryptographic key sizes none[20] that meet the following: **FIPS 180-4 [R39]**[21].

Application Note 24 *This SFR requires the TOE to implement the hash function SHA-1 as a cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [R26].*

6.2.5 FCS_COP.1/ENC

Cryptographic operation – Encryption/Decryption Triple DES

Hierarchical to: No other components.

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

FCS_COP.1.1/ENC:

The TSF shall perform secure messaging (BAC) – encryption and decryption[22] in accordance with a specified cryptographic

[18] [assignment: *list of cryptographic operations*]
[19] [selection: *SHA-1, SHA-224, SHA-256 or other approved algorithms*]
[20] [assignment: *cryptographic key sizes*]
[21] [selection: *FIPS 180-2 or other approved standards*]
[22] [assignment: *list of cryptographic operations*]

algorithm Triple-DES in CBC mode[23] and cryptographic key sizes 112 bits[24] that meet the following: NIST SP 800-67 [R37], NIST SP 800-38A [R38] and [R26] section 9.8[25].

Application Note 25 *FIPS 46-3 was withdrawn in 2005. The Triple Data Encryption Algorithm with 112 bit keys is still an NIST approved cryptographic algorithm as defined in NIST SP 800-67 [R37]. NIST SP 800-38A [R38] provides recommendation for block cipher modes.*

Application Note 26 *This SFR requires the TOE to implement the cryptographic primitive Triple-DES for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Mechanism according to the FCS_CKM.1 and FIA_UAU.4.*

6.2.6 FCS_COP.1/AUTH

Cryptographic operation – Authentication

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH:

The TSF shall perform symmetric authentication – encryption and decryption[26] in accordance with a specified cryptographic algorithm **AES**[27] and cryptographic key sizes: **256 bit**[28] that meet the following: **FIPS 197 [R40]**[29].

Application Note 27 *This SFR requires the TOE to implement the cryptographic primitive AES in CBC mode with 256-bit key according to [R40] for authentication attempt of a terminal*

---

[23] [assignment: *cryptographic algorithm*]
[24] [assignment: *cryptographic key sizes*]
[25] [assignment: *list of standards*]
[26] [assignment: *list of cryptographic operations*]
[27] [selection: *Triple-DES, AES*]
[28] [selection: 112, 128, 168, 192, 256]
[29] [selection: *FIPS 46-3, FIPS 197*]

as Initialization Agent in Step 6 Initialization of Phase 2 and as Personalization Agent in Step 7 Personalization of Phase 3, by means of the SCP03 mechanism (cf. FIA_UAU.4).

6.2.7 FCS_COP.1/MAC

Cryptographic operation – Retail MAC

Hierarchical to: No other components.

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

FCS_COP.1.1/MAC:

The TSF shall perform secure messaging – message authentication code[30] in accordance with a specified cryptographic algorithm Retail MAC[31] and cryptographic key sizes 112 bits[32] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [R32][33].

Application Note 28 *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.*

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

6.2.8 FCS_RND.1

Quality metrics for random numbers

Hierarchical to: No other components.

[30] [assignment: *list of cryptographic operations*]
[31] [assignment: *cryptographic algorithm*]
[32] [assignment: *cryptographic key sizes*]
[33] [assignment: *list of standards*]

Dependencies: No dependencies.

FCS_RND.1.1:

The TSF shall provide a mechanism to generate random numbers that meet **BSI AIS 20 DRG.3 quality metric [R3] (see Application Note 30)**[34].

Application Note 29 *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.*

Application Note 30 *The TOE makes use of the random number generator of the platform JCOP 4 P71 which is compliant with BSI AIS 20 [R3].*

6.3 Class FIA: Identification and authentication

Application Note 31 *Table 6-1 provides an overview on the authentication mechanisms used.*

Table 6-1 Overview of the authentication mechanisms used

Mechanism	SFR for the TOE	Algorithms and key sizes according to [R26]
Basic Access Control Authentication Mechanism	FIA_UAU.4 FIA_UAU.6 FIA_AFL.1/BAC	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Initialization Agent (SCP03)	FIA_UAU.4 FIA_AFL.1/Init	AES with 256-bit key (cf. FCS_COP.1/AUTH)
Symmetric Authentication Mechanism Personalization Agent (SCP03)	FIA_UAU.4 FIA_AFL.1/Pers	AES with 256-bit key (cf. FCS_COP.1/AUTH)

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

6.3.1 FIA_UID.1

Timing of identification

Hierarchical to: No other components.

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

Dependencies: No dependencies.

FIA_UID.1.1:

The TSF shall allow

- to read the IC Initialization Data in Phase 2 “Manufacturing”,
- to read the random identifier in Phase 3 “Personalization of the e-Document”,
- to read the random identifier in Phase 4 “Operational Use”[35]

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

FIA_UID.1.2:

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

Application Note 32 *In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role available for the TOE. The users in role Personalization Agent identify by themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.*

Application Note 33 *In the “Operational Use” phase the e-Document must not allow anybody to read the ICCSN, the e-Document identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the e-Document’s chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more than one RFID. If this identifier is randomly selected it will not violate the OT.Identification.*

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

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

6.3.2 FIA_UAU.1

Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1:

The TSF shall allow

- to read the IC Initialization data in Phase 2 "Manufacturing",
- to read the random identifier in Phase 3 "Personalization of the e-Document",
- to read the random identifier in Phase 4 "Operational Use"[36].

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

FIA_UAU.1.2:

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

Application Note 34 *The Basic Inspection System and the Personalization Agent authenticate themselves.*

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

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

6.3.3 FIA_UAU.4

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1:	

The TSF shall prevent reuse of authentication data related to

- Basic Access Control Authentication Mechanism,
- Authentication Mechanism based on **AES**[37].

Application Note 35 *The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [R26]. In the first step, the terminal authenticates itself to the e-Document's chip and the e-Document's chip authenticates to the terminal in the second step. In this second step, the e-Document's chip provides the terminal with a challenge-response-pair which allows a unique identification of the e-Document's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore, the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.*

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

6.3.4 FIA_UAU.5

Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1:	

The TSF shall provide

---

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

- Basic Access Control Authentication Mechanism,
- Symmetric authentication mechanism based on **AES**[38].

to support user authentication.

FIA_UAU.5.2:

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

- the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms: **the Symmetric Authentication Mechanism with Personalization keys Refinement: according to [R15],**
- the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys[39],

Refinement:

- **the TOE accepts the authentication attempt as Initialization Agent by the following mechanism: Symmetric Authentication Mechanism based on AES with Initialization key, according to [R15]**

Application Note 36 *The Symmetric Authentication Mechanism for the Initialization Agent and Personalization Agent are based on SCP03 protocol [R15] based on AES with 256-bit key.*

Application Note 37 *The authentication mechanisms for the Personalization Agent, as well as the Basic Access Control Mechanism include the secure messaging for all commands exchanged after successful authentication of the terminal.*

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

[38] [selection: *Triple-DES, AES or other approved mechanisms*]
[39] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

6.3.5 FIA_UAU.6

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1:

The TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism[40].

Application Note 38 *The Basic Access Control Mechanism specified in [R26] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.*

Application Note 39 *Note that in case the TOE should also fulfil [R5], the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process.*

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

6.3.6 FIA_AFL.1/Init

Authentication failure handling in Step 6 Initialization

Hierarchical to: No other components.

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

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Init:

The TSF shall detect when **<u>59</u>**[41] unsuccessful authentication attempts occur related to **<u>consecutive failed authentication attempts with respect to the Initialization key</u>** [42].

FIA_AFL.1.2/Init:

When the defined number of consecutive unsuccessful authentication attempts has been **<u>met</u>** the TSF shall **<u>allow only a limited set of commands</u>** [43].

Application Note 40 *The only allowed commands are "Get CLPC Data" and "Read attack counter log", managed by the Platform. The commands to open a SCP channel are no longer available (see section 5.9.2.1 of [R43]).*

6.3.7 FIA_AFL.1/Pers

Authentication failure handling in Step 8 "Personalization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Pers:

The TSF shall detect when **<u>59</u>**[44] unsuccessful authentication attempts occur related to **<u>consecutive failed authentication attempts with respect to the Personalization key</u>**[45].

[41] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[42] [assignment: list of authentication events]
[43] [assignment: *list of actions*]
[44] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[45] [assignment: list of authentication events]

FIA_AFL.1.2/Pers:

When the defined number of consecutive unsuccessful authentication attempts has been **met**[46], the TSF shall **allow only a limited set of commands** [47].

Application Note 41 *The only allowed commands are "Get CLPC Data" and "Read attack counter log", managed by the Platform. The commands to open a SCP channel are no longer available (see section 5.9.2.1 of [R43]).*

6.3.8 FIA_AFL.1/BAC

Authentication failure handling in Step 8 "Operational Use"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/BAC:

The TSF shall detect when **one**[48] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the BAC key**[49].

FIA_AFL.1.2/BAC:

When the defined number of consecutive unsuccessful authentication attempts has been **met**[50], the TSF shall **delay each following authentication attempt. The delay will be increased for each consecutive unsuccessful authentication** (cf. Application Note 43)[51].

Application Note 42 *After a successful authentication, the count is reset to zero.*

---

[46] [assignment: *met or surpassed*]
[47] [assignment: *list of actions*]
[48] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[49] [assignment: list of authentication events]
[50] [assignment: *met or surpassed*]
[51] [assignment: *list of actions*]

Application Note 43 *The value of the delay is configurable during the personalization step by the Personalization Agent.*

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

Subset access control* – Refinement: ~~Basic~~ *Access Control

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

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1:

The TSF shall enforce the **Refinement: ~~Basic~~** Access Control SFP[52] on terminals gaining write, read and modification access to:

- data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical e-Document,

Refinement:

- **TOE Initialization data, which include the Personalization key**,
- **TOE Personalization data, which include other TSF data**[53].

Application Note 44 *EF.DG15 is out of the scope of this SFR as Active Authentication is not included in the TOE.*

[52] [assignment: *access control SFP*]

[53] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

Basic security attribute based access control* – Refinement: ~~Basic~~ *Access Control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1:

The TSF shall enforce the **Refinement: ~~Basic~~** Access Control SFP[54] to objects based on the following:

- Subjects:
  - Personalization Agent,
  - Basic Inspection System,
  - Terminal,

  Refinement:
  - **Initialization Agent,**
- Objects:
  - data EF.DG1 to EF.DG16 of the logical e-Document,
  - data in EF.COM,
  - data in EF.SOD,

  Refinement:
  - **TOE Initialization data, which include the Personalization key**,
  - **TOE Personalization data, which include other TSF data.**
- Security attributes:

[54] [assignment: *access control SFP*]

- authentication status of terminals[55].

FDP_ACF.1.2:

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

- the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical e-Document[56],

Refinement:

- **the successfully authenticated Initialization Agent is allowed to write the personalization key of the logical e-Document,**
- **the successfully authenticated Personalization Agent is allowed to write the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16, as well as other TSF data, and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical e-Document.**

FDP_ACF.1.3:

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[57].

FDP_ACF.1.4:

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

- Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical e-Document.
- Any Terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical e-Document.

[55] [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*]
[56] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations or controlled objects*]
[57] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

- The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[58].

Application Note 45 *The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [R16] for details).*

Inter-TSF-Transfer

Application Note 46 *FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.*

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

6.4.3 FDP_UCT.1

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]

FDP_UCT.1.1:

The TSF shall enforce the Basic Access Control SFP[59] to be able to transmit and receive[60] user data in a manner protected from unauthorized disclosure.

[58] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[59] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[60] [selection: *transmit, receive*]

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

6.4.4 FDP_UIT.1

Data exchange integrity – e-Document

Hierarchical to: No other components.

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

FDP_UIT.1.1:

The TSF shall enforce the Basic Access Control SFP[61] to be able to transmit and receive[62] user data in a manner protected from modification, deletion, insertion and replay[63] errors.

FDP_UIT.1.2:

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[64] has occurred.

6.5 Class FMT: Security management

Application Note 47 *SFRs FMT_SMF.1 and FMT_SMR.1 provide basic requirements to 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).

---

[61] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[62] [selection: *transmit, receive*]
[63] [selection: *modification, deletion, insertion, replay*]
[64] [selection: *modification, deletion, insertion, replay*]

6.5.1 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,
- Personalization,

Application Note 48 *The ability to initialize and personalize the TOE is restricted to a successfully authenticated Initialization Agent or Personalization Agent by means of symmetric keys.*

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

6.5.2 FMT_SMR.1

Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1:

The TSF shall maintain the roles

- Manufacturer,
- Personalization Agent,
- Basic Inspection System[65].

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

FMT_SMR.1.2:

The TSF shall be able to associate users with roles.

Application Note 49 *The role Manufacturer collectively refers to the IC Manufacturer, the Card Manufacturer and the Initialization Agent.*

Application Note 50 *The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.*

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

6.5.3 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, and
- substantial information about construction of TSF to be gathered which may enable other attacks[66].

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

---

[66] [assignment: *limited capability and availability policy*]

6.5.4 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, and
- substantial information about construction of TSF to be gathered which may enable other attacks[67].

Application Note 51 *The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless, the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.*
Note that the term "software" in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application Note 52 *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.

---

[67] [assignment: *limited capability and availability policy*]

6.5.5 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[68] the Initialization Data and Pre-personalization Data[69] to the Manufacturer[70].

Application Note 53 *The initialization data may be classified into IC initialization data and TOE initialization data. IC initialization data include, but are not limited to, the authentication reference data for the Initialization Agent, which is the symmetric cryptographic initialization key. TOE initialization data include, but are not limited to, the authentication reference data for the Personalization Agent, which is the symmetric cryptographic personalization key.*

Application Note 54 *IC initialization data are written by the IC Manufacturer in Step 3, TOE initialization data are written by the Initialization Agent in Step 6, according to the life cycle described in section 1.5.*

6.5.6 FMT_MTD.1/INI_DIS

Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

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

FMT_MTD.1.1/INI_DIS:

---

68 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
69 [assignment: *list of TSF data*]
70 [assignment: *the authorised identified roles*]

The TSF shall restrict the ability to disable read access for users to[71] the Initialization Data[72] to the Personalization Agent[73].

6.5.7 FMT_MTD.1/KEY_WRITE

Management of TSF data – Key Write

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_WRITE:

The TSF shall restrict the ability to write[74] the Document Basic Access Keys[75] to the Personalization Agent[76].

6.5.8 FMT_MTD.1/KEY_READ/BAC

Management of TSF data – BAC keys and Personalization keys Read

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ/BAC:

The TSF shall restrict the ability to read[77] the Document Basic Access Keys and Personalization Agent Keys[78] to none[79].

---

[71] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[72] [assignment: *list of TSF data*]
[73] [assignment: *the authorised identified roles*]
[74] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[75] [assignment: *list of TSF data*]
[76] [assignment: *the authorised identified roles*]
[77] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[78] [assignment: *list of TSF data*]
[79] [assignment: *the authorised identified roles*]

6.5.9 FMT_MTD.1/KEY_READ/Init

Management of TSF data – Initialization key Read

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ/Init:

The TSF shall restrict the ability to read[80] the **Initialization key**[81] to none[82].

Application Note 55 *The Personalization Agent generates, stores, and ensures the correctness of the Document Basic Access Keys.*

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

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

6.6.1 FPT_EMSEC.1

TOE emanation

Hierarchical to: No other components.

[80] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[81] [assignment: *list of TSF data*]
[82] [assignment: *the authorised identified roles*]

Dependencies: No dependencies.

FPT_EMSEC.1.1:

The TOE shall not emit **electromagnetic and current emissions**[83] in excess of **intelligible threshold**[84] enabling access to Personalization Agent Key(s)[85] and **Initialization Key**[86].

FPT_EMSEC.1.2:

The TSF shall ensure any unauthorized users[87] are unable to use the following interface smart card circuits contacts[88] to gain access to Personalization Agent Key(s)[89] and **Initialization Key**[90].

Application Note 56 *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 origin from internal operation of the TOE or may origin 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 may provide either a smart card contactless interface or contacts according to ISO/IEC 7816-2 or both (both may be used by an attacker, even if not used even if not used by the terminal). 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).

83 [assignment: *type of emissions*]
84 [assignment: *specified limits*]
85 [assignment: *list of types of TSF data*]
86 [assignment: *list of types of user data*]
87 [assignment: *type of users*]
88 [assignment: *type of connection*]
89 [assignment: *list of types of TSF data*]
90 [assignment: *list of types of user data*]

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 out-of-range operating conditions where therefore a malfunction could occur,
- failure detected by TSF according to FPT_TST.1[91].

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

6.6.2 FPT_TST.1

TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1:

The TSF shall run a suite of self-tests **during initial start-up**[92]**, and at the conditions: when the applet is selected**[93] to demonstrate the correct operation of the TSF[94].

FPT_TST.1.2:

[91] [assignment: *list of types of failures in the TSF*]
[92] [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]*]
[93] [assignment: *conditions under which self-test should occur*]
[94] [selection: *[assignment: parts of TSF], the TSF*]

The TSF shall provide authorized users with the capability to verify the integrity of TSF data[95].

FPT_TST.1.3:

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

Application Note 57 *The Applet is automatically selected at the initial start-up. At the selection, the Applet checks that is running on the expected platform JCOP 4 P71, using a specific function provided by the platform. In case of failure, the Applet will raise a security exception to the platform.*

Application Note 58 *The Applet will check the attack logger on selection. In case the counter is zero, the Applet will raise a security exception to the platform.*

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

6.6.3 FPT_PHP.3

Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1:

The TSF shall resist physical manipulation and physical probing[96] to the TSF[97] by responding automatically such that the SFRs are always enforced.

Application Note 59 *The TOE will use appropriate countermeasures implemented by the IC manufacturer 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*

[95] [selection: *[assignment: parts of TSF data], TSF data*]
[96] [assignment: *physical tampering scenarios*]
[97] [assignment: *list of TSF devices/elements*]

response" means here (i) assuming that there might be an attack at any time, and (ii) countermeasures are provided at any time.

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 4 (EAL4), augmented by taking the component ALC_DVS.2.

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

Table 7-1 Security assurance requirements: EAL4 augmented with ALC_DVS.2

Assurance class	Assurance components
ADV *Development*	ADV_ARC.1 *Security architecture description*
	ADV_FSP.4 *Complete functional specification*
	ADV_IMP.1 *Implementation representation of the TSF*
	ADV_TDS.3 *Basic modular design*
AGD *Guidance documents*	AGD_OPE.1 *Operational user guidance*
	AGD_PRE.1 *Preparative procedures*
ALC *Life cycle support*	ALC_CMC.4 *Production support, acceptance procedures and automation*
	ALC_CMS.4 *Problem tracking CM coverage*
	ALC_DEL.1 *Delivery procedures*
	ALC_DVS.2 *Sufficiency of security measures*
	ALC_LCD.1 *Developer defined life-cycle model*
	ALC_TAT.1 *Well-defined development tools*
ASE *Security target evaluation*	ASE_CCL.1 *Conformance claims*
	ASE_ECD.1 *Extended components definition*
	ASE_INT.1 *ST introduction*
	ASE_OBJ.2 *Security objectives*

Assurance class	Assurance components
	ASE_REQ.2 *Derived security requirements*
	ASE_SPD.1 *Security problem definition*
	ASE_TSS.1 *TOE summary specification*
ATE *Tests*	ATE_COV.2 *Analysis of coverage*
	ATE_DPT.1 *Testing: basic design*
	ATE_FUN.1 *Functional testing*
	ATE_IND.2 *Independent testing - sample*
AVA *Vulnerability assessment*	AVA_VAN.3 *Focused vulnerability analysis*

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.AC_Init	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1					X				
FCS_CKM.1/BAC			X	X					
FCS_CKM.1/SCP		X	X						
FCS_CKM.4	X	X		X					
FCS_COP.1/SHA	X	X	X	X					
FCS_COP.1/ENC		X	X	X					
FCS_COP.1/AUTH	X	X	X						
FCS_COP.1/MAC		X	X	X					
FCS_RND.1		X	X	X					
FIA_UID.1				X	X				
FIA_AFL.1/Init					X				
FIA_AFL.1/Pers					X				
FIA_AFL.1/BAC				X	X				
FIA_UAU.1				X	X				
FIA_UAU.4	X	X	X	X					
FIA_UAU.5	X	X	X	X					
FIA_UAU.6			X	X					
FDP_ACC.1	X	X	X	X					
FDP_ACF.1	X	X	X	X					
FDP_UCT.1		X	X	X					
FDP_UIT.1		X	X	X					
FMT_SMF.1	X	X	X	X					
FMT_SMR.1	X	X	X	X					
FMT_LIM.1									X
FMT_LIM.2									X
FMT_MTD.1/INI_ENA					X				
FMT_MTD.1/INI_DIS					X				
FMT_MTD.1/KEY_WRITE		X	X	X					
FMT_MTD.1/KEY_READ/BAC		X	X	X					
FMT_MTD.1/KEY_READ/Init	X								

	OT.AC_Init	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FPT_EMSEC.1	X	X				X			
FPT_TST.1						X		X	
FPT_FLS.1	X	X				X		X	
FPT_PHP.3	X	X				X	X		

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 6, Initialization. The write access to the logical e-Document data are defined by the SFRs ***FDP_ACC.1*** and ***FDP_ACF.1*** as follows: only the successfully authenticated Initialization Agent is allowed to write the personalization key of the logical e-Document.
The authentication of the terminal as Initialization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4*** and ***FIA_UAU.5***. The Initialization Agent is authenticated by means of AES-256 cryptography (***FCS_COP.1/AUTH)*** with the Initialization key.
The SFR ***FMT_SMR.1*** lists the roles (including Initialization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Initialization). The SFR ***FMT_MTD.1/KEY_READ/Init*** prevents read access to the secret key of the Initialization Agent and ensures, together with the SFRs ***FCS_CKM.4***, ***FPT_EMSEC.1***, ***FPT_FLS.1***, and ***FPT_PHP.3***, the confidentiality of this 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 in Step 7 “Personalization". The write access to the logical e-Document data are defined by the SFRs ***FDP_ACC.1*** and ***FDP_ACF.1*** as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical e-Document only once.
The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4*** and ***FIA_UAU.5***. The Personalization Agent can be authenticated using the SCP03 mechanism based on AES (***FCS_CKM.1/SCP***, ***FCS_COP.1/SHA***, ***FCS_RND.1*** for key generation, and ***FCS_COP.1/AUTH***.
The SFRs ***FDP_UCT.1*** and ***FDP_UIT.1*** describe the protection of the transmitted data by means of secure messaging implemented by the SCP03 cryptographic functions according to the SFRs ***FCS_CKM.1/SCP***, ***FCS_COP.1/SHA***, ***FCS_RND.1*** for key generation, and ***FCS_COP.1/ENC*** as well as ***FCS_COP.1/MAC*** for encryption and MAC computation.
The SFR ***FMT_SMR.1*** lists the roles (including Personalization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Personalization) setting the Document Basic Access Keys according to the SFR ***FMT_MTD.1/KEY_WRITE*** as

authentication reference data. The SFR ***FMT_MTD.1/KEY_READ/BAC*** prevents read access to the secret key of the Personalization Agent and ensures, together with the SFRs ***FCS_CKM.4***, ***FPT_EMSEC.1***, ***FPT_FLS.1***, and ***FPT_PHP.3*** the confidentiality of this key. The SFR ***FCS_CKM.1/SCP*** allows to protect the transmitted data by means secure messaging during the personalization process.

Application Note 60 *The TOE does not allow the addition of data in the operational use phase. Therefore, the BAC mechanism is not used by the Personalization Agent.*

The security objective **OT.Data_Int** "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. The write access to the logical e-Document data is defined by the SFRs ***FDP_ACC.1*** and ***FDP_ACF.1*** in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical e-Document (***FDP_ACF.1.2***, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical e-Document (cf. ***FDP_ACF.1.4***). The SFR ***FMT_SMR.1*** lists the roles (including Personalization Agent) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFRs ***FIA_UAU.4***, ***FIA_UAU.5***, and ***FIA_UAU.6*** using either ***FCS_COP.1/ENC*** and ***FCS_COP.1/MAC*** or ***FCS_COP.1/AUTH***.

The security objective **OT.Data_Int** "Integrity of personal data" requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical e-Document data by means of the BAC mechanism. The SFRs ***FIA_UAU.6***, ***FDP_UCT.1***, and ***FDP_UIT.1*** requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to ***FCS_CKM.1/BAC*** (for the generation of the Document BAC keys), ***FCS_COP.1/SHA***, ***FCS_RND.1*** (for key generation), ***FCS_CKM.1/SCP*** (for the generation of the personalization keys), ***FCS_COP.1/ENC***, and ***FCS_COP.1/MAC*** (for encryption and MAC mode). The SFR ***FMT_MTD.1/KEY_WRITE*** requires the Personalization Agent to establish the Document Basic Access Keys in a way that they cannot be read by anyone in accordance to ***FMT_MTD.1/KEY_READ/BAC***.

The security objective **OT.Data_Conf** "Confidentiality of personal data" requires the TOE to ensure the confidentiality of the logical e-Document data groups EF.DG1 to EF.DG16. The SFRs ***FIA_UID.1*** and ***FIA_UAU.1*** allow only those actions before identification respective authentication which do not violate **OT.Data_Conf**. In case of failed authentication attempts, ***FIA_AFL.1/BAC*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical e-Document data is defined by ***FDP_ACC.1*** and ***FDP_ACF.1.2***: the successful authenticated Personalization Agent is allowed to read the data of the logical e-Document (EF.DG1 to EF.DG16). The successful authenticated Basic Inspection System is allowed to read the data of the logical e-Document

(EF.DG1, EF.DG2, and EF.DG5 to EF.DG16). The SFR ***FMT_SMR.1*** lists the roles (including Personalization Agent and Basic Inspection System) and the SFR ***FMT_SMF.1*** lists the TSF management functions (including Personalization for the key management for the Document Basic Access Keys).
The SFR ***FIA_UAU.4*** prevents reuse of authentication data to strengthen the authentication of the user. The SFR ***FIA_UAU.5*** enforces the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR ***FIA_UAU.6*** requests secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism, which includes the protection of the transmitted data in encryption and MAC mode by means of the cryptographic functions according to ***FCS_COP.1/ENC*** and ***FCS_COP.1/MAC*** (cf. the SFR ***FDP_UCT.1*** and ***FDP_UIT.1***, for key generation), ***FCS_COP.1/ENC***, and ***FCS_COP.1/MAC*** (for encryption and MAC mode). The SFRs ***FCS_CKM.1/BAC***, ***FCS_CKM.4***, ***FCS_COP.1/SHA***, and ***FCS_RND.1*** establish the key management for the secure messaging keys. The SFR ***FMT_MTD.1/KEY_WRITE*** addresses the key management, and ***FMT_MTD.1/KEY_READ/BAC*** prevents reading of the Document Basic Access Keys.
Note, neither the security objective **OT.Data_Conf**, nor the SFR ***FIA_UAU.5*** requires the Personalization Agent to use the Basic Access Control Authentication Mechanism or secure messaging.

The security objective **OT.Identification** “Identification and Authentication of the TOE” addresses the storage of the IC Identification Data uniquely identifying the e-Document’s chip in its non-volatile memory. This will be ensured by TSF according to SFR ***FAU_SAS.1***. Furthermore, the TOE shall identify itself only to a successful authenticated Basic Inspection System in Phase 4 “Operational Use”. The SFR ***FMT_MTD.1/INI_ENA*** allows only the Manufacturer to write Initialization Data (including the Personalization key). The SFR ***FMT_MTD.1/INI_DIS*** allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective **OT.Identification**. The SFRs ***FIA_UID.1*** and ***FIA_UAU.1*** do not allow reading of any data uniquely identifying the e-Document’s chip before successful authentication of the Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt (cf. Application Note 35). In case of failed authentication attempts, ***FIA_AFL.1/Init***, ***FIA_AFL.1/Pers*** shall allow only a limited set of commands, whilst ***FIA_AFL.1/BAC*** enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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_EMSEC.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.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/BAC	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ENC, FCS_COP.1/MAC Fulfilled by FCS_CKM.4
FCS_CKM.1/SCP	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/AUTH 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/BAC, And FCS_CKM.1/SCP
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	*Justification 1 for non-satisfied dependencies* Fulfilled by FCS_CMK.4

SFR	Dependencies	Support of the dependencies
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/BAC, FCS_CKM.1/SCP Fulfilled by FCS_CKM.4
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 2 for non-satisfied dependencies Partially fulfilled by FCS_CKM.4 Justification 2 for non-satisfied dependencies
FCS_COP.1/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/BAC, FCS_CKM.1/SCP Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	-
FIA_UID.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	-
FIA_UAU.5	No dependencies	-
FIA_UAU.6	No dependencies	-
FIA_AFL.1/Init	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/Pers	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/BAC	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1 *Justification 3 for non-satisfied dependencies*
FDP_UCT.1	[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]	*Justification 4 for non-satisfied dependencies* Fulfilled by FDP_ACC.1
FDP_UIT.1	[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]	*Justification 4 for non-satisfied dependencies* Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
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
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
FMT_MTD.1/KEY_READ/ BAC	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1

SFR	Dependencies	Support of the dependencies
FMT_MTD.1/KEY_READ/Init	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FPT_TST.1	No dependencies	-

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

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

Justification 2: The SFR FCS_COP.1/AUTH refers to the symmetric Initialization Key and Personalization Key. All two keys are permanently stored, respectively, during IC manufacturing and initialization (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 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.

Justification 3: The access control TSF according to FDP_ACF.1 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 4: The SFRs FDP_UCT.1 and FDP_UIT.1 require the use of secure messaging between the e-Document and the BIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels, since there is only one channel. Since the TOE does not provide a direct human interface, a trusted path as required by FTP_TRP.1 is not applicable here.

8.3 Security assurance requirements rationale

The EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The TOE assurance level is augmented with respect to the EAL4 package for what refers to development security (ALC_DVS.2 instead of ALC_DVS.1).

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

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 8.1 "Dependency rationale" 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-satisfied dependencies are appropriately explained.

The assurance class EAL4 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 8.1 "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. See Application Note 19.
FCS_CKM.1/BAC	The TOE generates session keys for Secure Messaging soon after a successful BAC authentication of the Basic Inspection System, as described in Appendix D.1 of ICAO Doc 9303/11 [R26]. See Application Note 20.
FCS_CKM.1/SCP	The TOE generates session keys for Secure Messaging soon after a successful authentication of the Personalization Agent, as described in [R15]. See Application Note 21.
FCS_CKM.4	Session keys are overwritten with zeros when a Secure Messaging session is closed. See Application Note 22.
FCS_COP.1/SHA	The TOE implements the digesting algorithms SHA-1. See Application Note 24.
FCS_COP.1/ENC	During a Secure Messaging session, 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. See Application Note 26.
FCS_COP.1/AUTH	The TOE provides the SCP03 mechanism to authenticate the Initialization Agent and the Personalization Agent according to [R15]. See also Application Note 27.

Security functional requirement	Implementation
FCS_COP.1/MAC	During a Secure Messaging session, 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 Retail MAC algorithm and cryptographic key sizes 112 bit according to ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2. See Application Note 28.
FCS_RND.1	The TOE generates random numbers for use in the SCP03 protocol and BAC authentication. See also Application Note 29 and Application Note 30.
FIA_UID.1	The TOE applies access control policies to guarantee that: • access to the initialization data and to the random identifier for contactless protocol is allowed before users are identified, • read access to any other data requires a successful execution of SCP03 protocol (in Personalization) or BAC protocol (in the operational use phase). The required access privileges are set for each data set by the agent that writes the related persistent object. See Application Note 32 and Application Note 33.
FIA_UAU.1	The TOE applies access control policies to guarantee that read access to data, in each TOE life cycle phase, is given to authorized users only. Initialization data and the random identifier for contactless protocol, can be accessed without any authentication. Read access in Personalization requires a successful completion of the SCP03 protocol. Read access in the operational use phase requires a BAC authentication. The required access privileges are set for each data set by the agent that writes the related persistent object. See Application Note 34.
FIA_UAU.4	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 35.

Security functional requirement	Implementation
FIA_UAU.5	The TOE provides: • the BAC mechanism to authenticate the user in the operational use phase with 112-bit BAC keys, • the SCP03 protocol to authenticate the Initialization Agent with a 256-bit Initialization key, • the SCP03 protocol to authenticate the Personalization Agent with a 256-bit Personalization key, See Application Note 36 and Application Note 37
FIA_UAU.6	Secure Messaging established after a successful BAC authentication provides re-authentication of the user.
FIA_AFL.1/Init	In case of unsuccessful authentication, the Initialization Agent has only a limited number of consecutive authentication attempts after which only a limited set of commands is allowed. The maximum number of unsuccessful consecutive authentications is set to 59.
FIA_AFL.1/Pers	In case of unsuccessful authentication, the Personalization Agent has only a limited number of consecutive authentication attempts after which only a limited set of commands is allowed. The maximum number of unsuccessful consecutive authentications is set to 59.
FIA_AFL.1/BAC	When an unsuccessful BAC authentication happens, the next authentication will be delayed and the delay will be increased for each consecutive unsuccessful BAC authentication to counter brute force attacks. The delay will be reset after the next first successful authentication. See Application Note 42.
FDP_ACC.1	The TOE is configured for usage with Basic Inspection Systems only. See also Application Note 44.

Security functional requirement	Implementation
FDP_ACF.1	The TOE keeps a security status for each data object to guarantee that: • EF.COM, EF.SOD, EF.DG1 to EF.DG14, EF.DG.16 can be accessed for reading and writing by a successfully authenticated Personalization Agent only, • EF.COM, EF.SOD, EF.DG1, EF.DG.2, EF.DG5 to EF.DG14 and EF.DG16 can be accessed for reading by a successfully authenticated Basic Inspection System only. The TSF checks the security status is checked before any access to the protected data. See Application Note 45.
FDP_UCT.1	The TOE protects data confidentiality of received and transmitted data by means of Triple-DES cryptography within Secure Messaging sessions in MAC-ENC mode.
FDP_UIT.1	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.
FMT_SMF.1	The TOE provides features for storing Initialization data, Personalization Data and Configuration Data, ensuring that only the entitled agents are able to do so. See Application Note 48.
FMT_SMR.1	The TOE distinguishes between the roles IC Manufacturer, Initialization Agent, Personalization Agent and Basic Inspection System, and grants each of them the access privileges allowed by the security policies. All the above roles are implicitly identified via the corresponding authentication key. See Application Note 49.
FMT_LIM.1	The test features of the Applet, as well as the authentication mechanism granting access to them, are permanently disabled in the evaluated configuration of the Applet. As regards the test features of the Platform, information on their limitation is provided in the TOE summary specification of the public security target for platform SFRs FMT_LIM.1, FMT_LIM.2 [R41].
FMT_LIM.2	As specified for SFR FMT_LIM.1.

Security functional requirement	Implementation
FMT_MTD.1/INI_ENA	The access control policy enforced by the TOE guarantees that in the Initialization only the entitled agent can write data. The TSF checks the possess of access privileges before any access is made. See Application Note 53 and Application Note 54.
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/KEY_WRITE	The access control policy enforced by the TOE guarantees that e-Document BAC keys can be written by the Personalization Agent only. The TSF checks the possess of access privileges before any access is made to those keys.
FMT_MTD.1/KEY_READ/BAC	The property defining read access conditions of the Document BAC keys and of the Personalization Agent keys are set, when those keys are written, so that the keys cannot be read by anyone under any circumstances. The TSF checks the access privileges before any access is made to those keys.
FMT_MTD.1/KEY_READ/Init	The property defining read access conditions of Initialization Agent key is set when that key is written, so that the key cannot be read by anyone under any circumstances. The TSF checks the access privileges before any access is made to that key.
FPT_EMSEC.1	Leakage of confidential data through side channels is prevented by the security features of the platform and application, in accordance with the security recommendations contained in the Platform guidance documentation [R43].
FPT_FLS.1	In case self-test fails or a physical attack is detected, the Applet enters an endless loop, so that all cryptographic operations and data output interfaces are inhibited.
FPT_TST.1	During initial start-up, the Applet automatically is selected, and it checks that it is running on the expected platform JCOP 4 P71, using a specific function provided by the platform. The attack logger is checked too. Furthermore at the initial start-up the platform performs self-checks as described in [R43]
FPT_PHP.3	Detection of physical attacks is ensured by the security features of the Platform.

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 [R10].
The implementation is based on a description of the security architecture of the TOE and on an informal 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 preparation guidance. The latter document also addresses the family AGD_PRE.

The necessary information for the e-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 user. 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 in 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 HIDApp-eDoc suite
ADV_FSP.4	Functional Specification for HIDApp-eDoc suite
ADV_IMP.1	Source code of HIDApp-eDoc suite
ADV_TDS.3	Design Description for HIDApp-eDoc suite
AGD_OPE.1	Operational User Guidance for HIDApp-eDoc suite
AGD_PRE.1	Initialization Guidance for HIDApp-eDoc suite Personalization Guidance for HIDApp-eDoc suite
ALC_CMC.4, ALC_CMS.4	Configuration management plan for Smart Cards and Embedded Software Configuration list for HIDApp-eDoc suite Evidences of configuration management
ALC_DEL.1	Secure delivery procedure for HIDApp-eDoc suite Delivery documentation
ALC_DVS.2	Development Security for Smart Cards and Embedded Software - description Development Security for Smart Cards and Embedded Software - documentation
ALC_LCD.1	Life Cycle Definition for Smart Cards and Embedded Software
ALC_TAT.1	Tools and Techniques for HIDApp-eDoc suite

Security assurance requirements	Documents
ATE_COV.2	Test Coverage Analysis for HIDApp-eDoc suite
ATE_DPT.1	Test Depth Analysis for HIDApp-eDoc suite
ATE_FUN.1	Functional Test Plan for HIDApp-eDoc suite Evidences of tests
ATE_IND.2	Documentation related to the independent test
AVA_VAN.3	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
ASCII	American Standard Code for Information Interchange
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication/Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DPA	Differential Power Analysis
DS	Document Signer
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EF	Elementary File
EIS	Extended Inspection System
FID	File Identifier
GIS	General Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
ICCSN	Integrated Circuit Card Serial Number
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
PIS	Primary Inspection System
PKI	Public Key Infrastructure
PP	Protection Profile
QSCD	Qualified Signature Creation Device
RFID	Radio Frequency Identification
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
TSF	TOE Security Functionality
TSP	TOE Security Policy
VIZ	Visual Inspection Zone

10.2 Glossary

Term	Definition
Active Authentication (AA)	Security mechanism defined in ICAO Doc 9303 [R26], 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.
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.
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 [R26] by which means the e-Document's chip proves and the inspection system protects their communication by means of secure messaging with the Document BAC Keys.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the BAC Mechanism and authenticates themselves to the e-Document's chip using the Document BAC Keys derived from the printed MRZ data for reading the logical e-Document.
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 of an e-Document [R25].
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.
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.
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 Eighth Edition, 2021 **[R27]**.
Country Signing Certification Authority Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (PKCSCA) issued by the Country Signing Certification Authority and stored in the inspection system.

Term	Definition
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 [R26]. 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 [R26].
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 [R29], 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}) [R25] Eighth Edition, 2021 **[R27]**.
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 Eighth Edition, 2021 **[R27]**. This role is usually delegated to a Personalization Agent.
e-Document	An official document of identity issued by a State or Organization, which may be used by the rightful holder.
e-Document Application	Non-executable data defining the functionality of the operating system on the IC as the e-Document's chip. It includes: i. the file structure implementing the LDS [R25], ii. the definition of the User Data, but does not include the User Data themselves (i.e. content of EF.DG1 to EF.DG 16), and iii. the TSF Data including the definition of the authentication data, but without the authentication data themselves.
e-Document Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the e-Document's chip based on MRZ information as a key seed and access condition to data stored on e-Document's chip according to LDS.
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 [R34] [R35] and programmed according to the Logical Data Structure as specified by ICAO [R25].
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

Term	Definition
	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 enhanced-basic 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 [R25].
Extended Access Control (EAC)	Security mechanism identified in BSI TR-03110 [R6] [R7] 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 [R25].
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

Term	Definition
	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 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 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 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 [R25]. 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 [R25] 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 international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read [R25].
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 [R25].
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 [R25].
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.
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 [R26] Eighth Edition, 2021 **[R27]**.
Personalization	The process by which the portrait, signature, and biographical data are applied to the document. This may also include the optional biometric data collected during the enrolment.

Term	Definition
Personalization Agent	The agent delegated by the Issuing State or Organization to personalize the e-Document for the holder by: i. establishing the identity of the holder for the biographic data in the e-Document, ii. enrolling the biometric reference data of the e-Document holder i.e. the portrait, the encoded finger image(s) or the encoded iris image(s), and iii. writing these data on the physical and logical e-Document for the holder.
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): i. biographical data, ii. data of the Machine Readable Zone, iii. photographic image, and iv. other data.
Presenter	Person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the contact or contactless communication with the e-Document's chip and does not implement the terminal's part of the Basic Access Control Mechanism.
Random Identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the e-Document, thus participates in the prevention of traceability.
Receiving State or Organization	The Country or the Organization to which the e-Document holder is applying for entry or control [R25].
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.
Secure Messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R31].

Term	Definition
Skimming	Imitation of the inspection system to read the logical e-Document or parts of it via the contact or contactless communication channels of the TOE without knowledge of the printed MRZ data.
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.
TSF Data	Data created by and for the TOE that might affect the operation of the TOE [R8].
User Data	Data created by and for the user that does not affect the operation of the TSF [R8].
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 [R25].
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] ACSIEL: *Technical Report - Signature creation and administration for eIDAS Token, Version 1.0, July 2015*

[R2] BSI: *Certification Report BSI-DSZ-CC-1136-V3-2022 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 7 September 2022*

[R3] BSI: *Functionality classes for random number generators, AIS20/31, Version 2.0, 18 September 2011.*

[R4] 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*

[R5] 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*

[R6] 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*

[R7] 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*

[R8] 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*

[R9] 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*

[R10] 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*

[R11] European Parliament: *Regulation (EU) No 910/2014 of the European Parliament and of the Council, 23 July 2014*

[R12] European Parliament: *Commission Implementing Decision (EU) 2016/650, 25 April 2016*

[R13] European Parliament: *Directive 1999/93/EC on a Community framework for electronic signatures, December 1999*

[R14] GlobalPlatform: *GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015*

[R15] GlobalPlatform: *GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v 2.2 - Amendment D v1.1.1, July 2014.*

[R16] HID Global: *Security Target for HIDApp-eDoc suite – ICAO Application* **–** *EAC-PACE-AA, v. 1.6, ref. TCAE210002*

[R17] HID Global: *Security Target for HIDApp-eDoc suite – ICAO Application – Basic Access Control, v. 1.6, ref. TCAE210001*

[R18] HID Global: *Security Target for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.5, ref. TCAE210003*

[R19] HID Global: *Initialization Guidance for HIDApp-eDoc suite, v. 1.4, ref. TCAE210007*

[R20] HID Global: *Personalization Guidance for HIDApp-eDoc suite – ICAO Application, v. 1.6, ref. TCAE210008*

[R21] HID Global: *Personalization Guidance for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.6, ref. TCAE210009*

[R22] HID Global: *Operational User Guidance for HIDApp-eDoc suite – ICAO Application, v. 1.5, ref. TCAE210010*

[R23] HID Global: *Operational User Guidance for HIDApp-eDoc suite – eIDAS eSign Application, v. 1.5, ref. TCAE210011*

[R24] HID Global: *Secure Delivery Procedure for HIDApp-eDoc suite, ref. TCAE210012*

[R25] 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), Eighth Edition, 2021*

[R26] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs, Eighth Edition, 2021*

[R27] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs, Eighth Edition, 2021*

[R28] IETF Network Working Group: *Request For Comments 2119, Key words for use in*

RFCs to Indicate Requirement Levels, March 1997

[R29] IETF Network Working Group: *Request For Comments 3369, Cryptographic Message Syntax (CMS), August 2002*

[R30] ISO/IEC: *International Standard 7816-2, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimensions and location of the contacts*

[R31] ISO/IEC: *International Standard 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*

[R32] ISO/IEC: *International Standard 9797-1, Information Technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

[R33] ISO/IEC: *International Standard 11770-2, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

[R34] ISO/IEC: *International Standard 14443-3, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision*

[R35] ISO/IEC: *International Standard 14443-4, Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*

[R36] JIWG: *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018*

[R37] NIST: *Special Publication 800-67 Revision 2, Recommendation for the Triple Data Encryption Standard (TDEA) Block Cipher, November 2017*

[R38] NIST: *Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, December 2001*

[R39] NIST: *FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012*

[R40] NIST: *FIPS PUB 197, Federal Information Processing Standards Publication, Advanced Encryption Standard (AES), November 2001*

[R41] NXP: *JCOP 4 P71, Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.11 – 03 January 2023*

[R42] NXP: *NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite Rev. 2.6 – 13 June 2022.*

[R43] NXP: *JCOP 4 P71, User manual for JCOP 4 P71, Rev. 4.3, DocNo 469543, 08 September 2022, NXP Semiconductors.*

[R44] Oracle: Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5, May 2015

[R45] Oracle: *Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015*

[R46] Oracle: *Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015*

[R47] TUV: *Certification Report NSCIB-CC-180212-5MA1 for JCOP 4 P71 from NXP Semiconductors Germany GmbH, 23 January 2023*

Appendix A Platform identification

The platform on which the TOE is based (cf. [R36]) is the NXP JCOP 4 P71.

The platform includes:

- The certified microcontroller NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (cf. [R2])
- The Security IC Dedicated Software, composed by:
  - MC FW (Micro Controller Firmware) [R42]
  - Crypto Library [R42]
- The Security IC Embedded Software, composed by
  - JCOP 4 P71 OS, consisting of:
    - JCVM, JCRE and JCAPI implemented according to Java Card Specification Version 3.0.5 Classic
    - GP framework implemented according GlobalPlatform Version 2.3 and Amendment D, Secure Channel Protocol ’03’ Version 1.1.1
- Additionally proprietary APIs, described in the document [R43].

The TOE configuration used for the TOE HIDApp-eDoc is the Configuration Banking & Secure ID, JCOP 4 P71 v4.7 R1.01.4.

The platform has obtained a Common Criteria certification at Evaluation Assurance Level EAL6 augmented by ASE_TSS.2 and ALC_FLR.1:

- Certification ID: NSCIB-CC-180212-5MA1
- Security Target: [R41]
- Certification Report: [R47]

END OF DOCUMENT