www.hidglobal.com

www.arjo-systems.com

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

SOMA-c007 Machine Readable Electronic Document

Security Target
ICAO Application
Basic Access Control

Public Version

Common Criteria version 3.1 revision 4
Assurance Level EAL4+

Version	1.0
Date	2017-09-21
Reference	TCAE160019
Classification	PUBLIC

Table of Contents

List of Tables

List of Figures

Abbreviations and Notations

Numerical values

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

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

Denoted text

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

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

Example: e-Document instead of MRTD.

Key words

The words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” are to be interpreted as described in RFC2119 [R24].

Diagram legend

The following legend applies to the diagrams that illustrate the high-level objects present in the TOE persistent memory at the completion of the various stages of the TOE life cycle (cf. section 1.5):

📁	Dedicated File *not modified in the current stage*	📁	Dedicated File *created in the current stage*
■	System Object *not modified in the current stage*	□	Elementary File *not modified in the current stage*
■	System Object *modified in the current stage*	□	Elementary File *modified in the current stage*
■	System Object *optionally/conditionally modified in the current stage*	□	Elementary File *optionally/conditionally modified in the current stage*
■	System Object *created in the current stage and filled*	□	Elementary File *created in the current stage and filled*
E	System Object *created in the current stage and left empty*	E	Elementary File *created in the current stage and left empty*
🚫	System Object *no longer available*	🚫	Elementary File *no longer available*
▨	System Object *optional/conditional*	▨	Elementary File *optional/conditional*

1. Introduction

1.1 ST overview

This Security Target (ST) document defines the security objectives and requirements, as well as the scope of the Common Criteria evaluation of SOMA-c007 Machine Readable Electronic Document.

The Target Of Evaluation (TOE) is the integrated circuit chip Infineon *M7892 G12* equipped with the operating system SOMA-c007 and with e-Document applications, namely an International Civil Aviation Organization (ICAO) application compliant with ICAO Doc 9303 [R22][R23], and a Secure Signature Creation Device (SSCD) application compliant with European Commission Directive 1999/93/ec [R20]. The SSCD application can optionally be configured as a PKCS #15 application [R40].

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.

This ST addresses the Basic Access Control (BAC) security mechanism, featured by the ICAO application according to ICAO Doc 9303 [R23].

The ICAO application also supports the following advanced security methods:

- Extended Access Control (EAC), which includes Chip Authentication according to ICAO Doc 9303 7th ed. Part 11 [R23], and Terminal Authentication according to BSI TR-03110 [R14][R15],
- Password Authenticated Connection Establishment (PACE), according to ICAO Doc 9303 7th ed. Part 11 [R23] and
- Active Authentication according to ICAO Doc 9303 7th ed. Part 11 [R23]

which are addressed by another ST [R1].

The SSCD application requirements are addressed by still another ST [R2].

1.2 ST reference

Table 1-1 ST reference

Title	Security Target SOMA-c007 Machine Readable Electronic Document - ICAO Application - Basic Access Control - Public Version
Version	1.0
Authors	Marco EVANGELISTA, Pasquale NOCE
Reference	TCAE160019

1.3 TOE reference

Table 1-2 TOE reference

TOE name	SOMA-c007 Machine Readable Electronic Document Basic Access Control
TOE version	2
TOE developer	HID Global/Arjo Systems
TOE identifier	SOMA-c007_2
TOE identification data	53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 37h 5Fh 32h

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

SOMA-c007_2
(ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 30h 37h 5Fh 32h)

where:

- “SOMA-c007” is the product name,
- the underscore character is a separator, and
- “2” is the TOE version number.

The ASCII encoding of the TOE identifier constitutes the TOE identification data, located in the persistent memory of the chip. Instructions for reading these data are provided by the guidance documentation [R3] [R4] [R5] [R6].

1.4 TOE overview

1.4.1 TOE definition

The TOE is the integrated circuit chip of machine readable electronic documents programmed according to the Logical Data Structure (LDS) [R22] and providing the Basic Access Control (BAC) according to ICAO Doc 9303 7th edition Part 11 [R23].

The TOE is composed of:

- the circuitry of the dual-interface e-Document's chip Infineon *M7892 G12* (see Appendix A),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the smart card operating system SOMA-c007,
- an ICAO application compliant with ICAO Doc 9303-10 [R22] and Doc 9303-11 [R23],
- a SSCD application compliant with European Parliament Directive 1999/93/EC [R20] (this application is not in the scope of this ST),
- the associated guidance documentation [R3] [R4] [R5] [R6].

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

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 [R11].

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[1] 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.

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 [R12] 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[2];
  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.*

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

[2] These biometric reference data are optional according to [R16]. These data are protected by means of extended access control, which is out of scope of this ST.

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 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 mechanism requiring decrypting of a cryptogram by means of AES 256 cryptography, until completion of the initialization process. After completion, the decryption of the cryptogram is no longer possible.

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

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

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

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

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 the Active Authentication and the 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 [R23], 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 application. Note, the substrate holding the chip as well as the antenna (if any) 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 described in terms of the following four life cycle phases, each divided in one or more steps:

1. Phase 1: Development, composed of
   Step 1) the development of the operating system software by the Embedded Software Developer and
   Step 2) the development of the integrated circuit by the IC Manufacturer;

2. Phase 2: Manufacturing, composed of
   Step 3) the fabrication of the integrated circuit by the IC Manufacturer,
   Step 4) the embedding of the chip in a substrate with an antenna. The antenna may be omitted if the IC contacts are exposed.
   Step 5) the initialization and OS configuration and
   Step 6) the pre-personalization of the e-Document;

3. Phase 3: Personalization, comprising
   Step 7) Personalization of the e-Document for the holder

4. Phase 4: Operational Use, comprising
   Step 8) Inspection of the e-Document

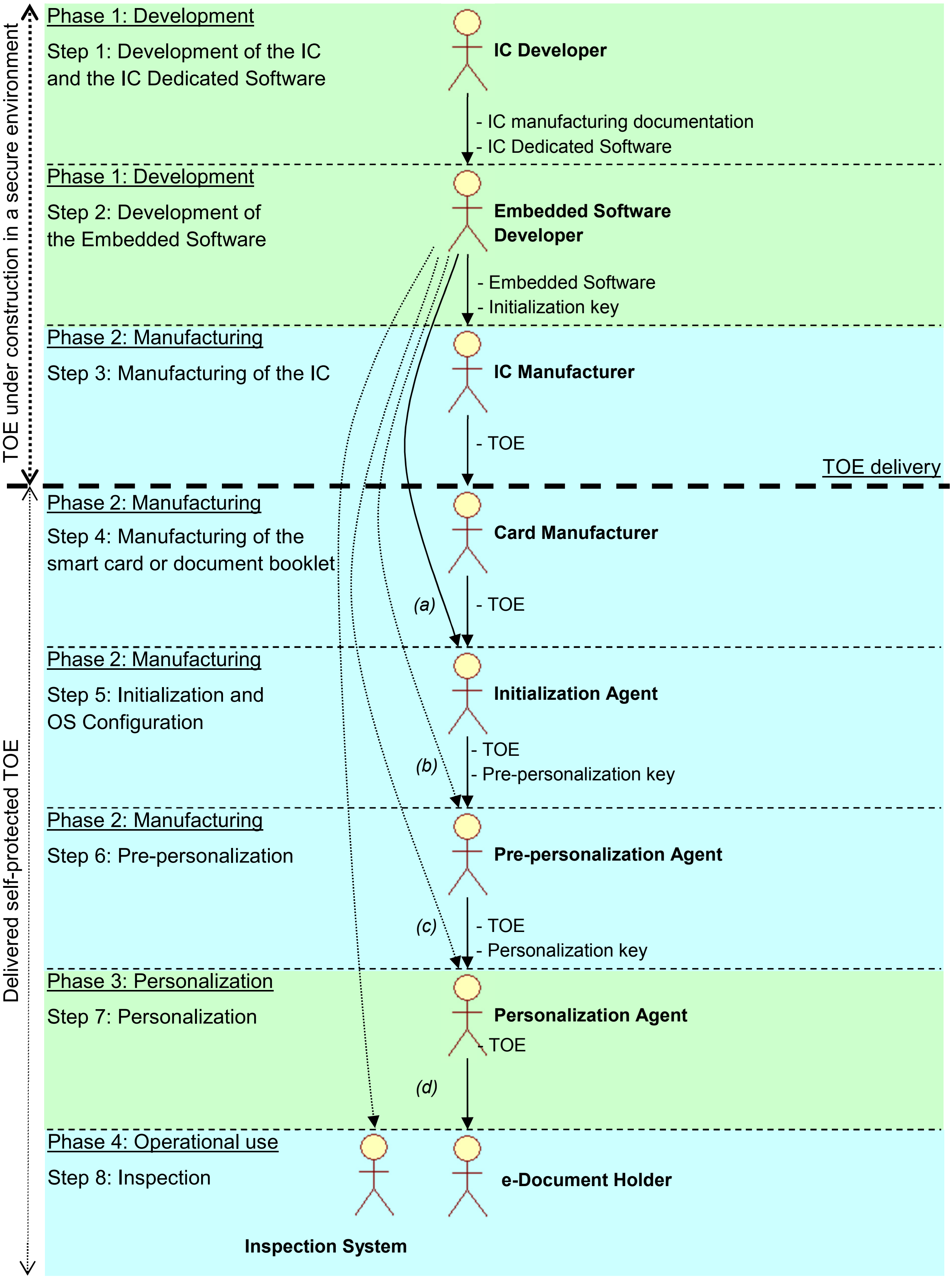
Application Note 2 *The entire Development phase, as well as Step 3 "fabrication of the* *integrated circuit" of the Manufacturing phase are the only phases covered by assurance as during these phases the TOE is under construction in a protected environment.*

Figure 1-1 shows life cycle phases and steps. The picture also identifies the actors involved in each life cycle step. Direct deliveries of items between actors are represented with continuous lines, while deliveries in which intermediate actors may be in charge of receiving the exchanged items and forwarding them to the subsequent actors are represented with dotted lines.
Deliveries of items not occurring between 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 not occurring between consecutive actors

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

Figure 1-1 TOE life cycle



Detailed information about the operations available in each life cycle phase of the TOE is provided in the guidance documentation.
Table 1-4 identifies the roles in each phase of the TOE life cycle.

Table 1-4 Roles Identification

Phase	Role	Identification	Data loaded
1	IC Developer	Infineon	N/A
1	Embedded Software Developer	Arjo Systems	N/A
2	IC Manufacturer	Infineon	Initialization key Initial data for internal objects.
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.	N/A
2	Initialization Agent	The agent who is acting on behalf of the Issuing State or Organization to configure the OS and load the Pre-personalization key.	Initial OS parameters (initialization cryptogram). Further details are provided by the Initialization Guidance [R3].
2	Pre-personalization Agent	The agent who is acting on behalf of the Issuing State or Organization to assemble the document book embedding the TOE, and to pre-personalize the e-Document	Personalization keys, Chip Authentication keys, Active Authentication keys, Initial LDS configuration. Further details are provided by the Pre-personalization Guidance [R4].
3	Personalization Agent	The agent who is acting on the behalf of the Issuing State or Organization to personalize the e-Document for the holder	PACE keys, BAC keys, Trustpoint, Certificates, Initial LDS configuration. Further details are provided by the Personalization Guidance [R5].
4	e-Document Holder	The rightful owner of the e-Document	N/A

Phase	Role	Identification	Data loaded
	e-Document Manufacturer	Role that collectively identifies the Initialization Agent and the Pre-personalization Agent.	N/A
	Manufacturer	Role that collectively identifies the roles acting in Phase 2, i.e. IC Manufacturer, Card Manufacturer and Pre-personalization Agent.	N/A

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

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

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

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

1.5.1 Phase 1: Development

(Step 1) The **IC Developer** develops the integrated circuit, the IC Dedicated Software, and the guidance documentation associated with these TOE components.

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

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

(Step 2) The **Embedded Software Developer** uses the guidance documentation for the integrated circuit and for relevant parts of the IC Dedicated Software and develops the Embedded Software (consisting of the operating system, the ICAO application, and the

SSCD application), as well as the guidance documentation associated with these TOE components.

Furthermore, the **Embedded Software Developer** generates the initialization key and the pre-personalization key, and makes use of the former key to encrypt the latter one, as well as (optionally) a bitmap encoding configuration data for the operating system.

Finally, the following items are securely delivered to the **IC Manufacturer**:

- the Embedded Software,
- the initialization key.

Moreover, the cryptograms enciphered using the initialization key are securely delivered to the **Initialization Agent**, while the pre-personalization key is securely delivered to either the **Initialization Agent** or the **Pre-personalization Agent**.
As regards TOE guidance documentation, either all documents are securely delivered to the **Initialization Agent**, or each document is securely delivered to the recipient actors as identified in Table 1-5.

1.5.2 Phase 2: Manufacturing

(Step 3) The **IC Manufacturer** produces the TOE integrated circuit, containing the IC Dedicated Software and the Embedded Software, and creates in the IC persistent memory the high-level objects.
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 3, i.e. with the delivery of the TOE from the IC Manufacturer to the Card Manufacturer, in the form of an IC not yet embedded. That is to say, this is the event upon which the construction of the TOE in a secure environment ends, and the TOE begins to be self-protected.*

(Step 4) The **Card Manufacturer** embeds the programmed IC into a plastic or paper substrate, optionally equipping it with an antenna (for ISO 14443 interface), and optionally exposing IC contacts (for ISO 7816-2 interface).

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

(Step 5) The **Initialization Agent** sends the encrypted configuration data (if any), as well as the encrypted pre-personalization key, to the TOE. Then, the TOE deciphers the cryptograms using the initialization key, verifies the correctness of the resulting plaintexts, and stores the data into persistent memory.

Application Note 4 *During TOE initialization, the Initialization Agent establishes a trusted channel with the TOE through a GIM authentication, which consists of sending the configuration data (if any) and the pre-personalization key, encrypted with the initialization key, to the TOE. For further information, cf. the initialization guidance [R3].*

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

(Step 6) The **Pre-personalization Agent** generates the personalization key, and then creates/modifies the high-level objects relevant for the ICAO application in the IC persistent memory.

Application Note 5 *In this step the Pre-personalization Agent shall perform a mutual authentication using the Pre-personalization keys (stored by the Initialization Agent in Step 5).*

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

1.5.3 Phase 3: Personalization

(Step 7) The personalization of the e-Document 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.

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

(i) the digital MRZ data (EF.DG1),
(ii) the digitized portrait (EF.DG2), and
(iii) the Document security object.

The signing of the Document security object by the Document signer [R22] finalizes the personalization of the genuine e-Document for the document holder.

Application Note 6 *The authenticated Personalization Agent shall additionally verify an Application Secret Code (ASC$_{RASD}$) to have read access to some user data stored in Step 6.*

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

Application Note 7 *The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [R16], section 92) comprise (but are not limited to) the Initialization key, the Pre-personalization key, the Personalization key and the Basic Access Control Key.*

Application Note 8 *This security target distinguishes between the Personalization Agent as an entity known to the TOE and the Document Signer as an entity in the TOE IT environment signing the Document security object as described in [R22]. This approach allows but does not enforce the separation of these roles.*

1.5.4 Phase 4: Operational use

(Step 8) “Inspection of the e-Document”
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 according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State, but they can never be modified.

Application Note 9 *This ST considers the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore defines the TOE delivery according to CC after this phase. 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. Nevertheless, the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.*

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures, after TOE delivery up to the "Operational Use" (phase 4) have to be considered in the product evaluation process under AGD assurance class. Therefore this security target outlines the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery.
Some production steps, e.g. Step 6 in Phase 2 may also take place in the Phase 3.

1.6 TOE Description

1.6.1 Physical scope of the TOE

The physical TOE is comprised of the following parts:

- the integrated circuit chip *M7892 G12* (microcontroller) programmed with the operating system and with the ICAO application (Embedded Software).
- the guidance documentation, composed by:
    - the Initialization Guidance [R3] for the Initialization Agent,
    - the Pre-personalization guidance [R4] for the Pre-personalization Agent,
    - the Personalization Guidance [R5] for the Personalization Agent, and
    - The Operational User Guidance [R6] for the User (Inspection System).

The Embedded Software of the TOE comprises the following software components stored in the non-volatile memory units of the microcontroller:

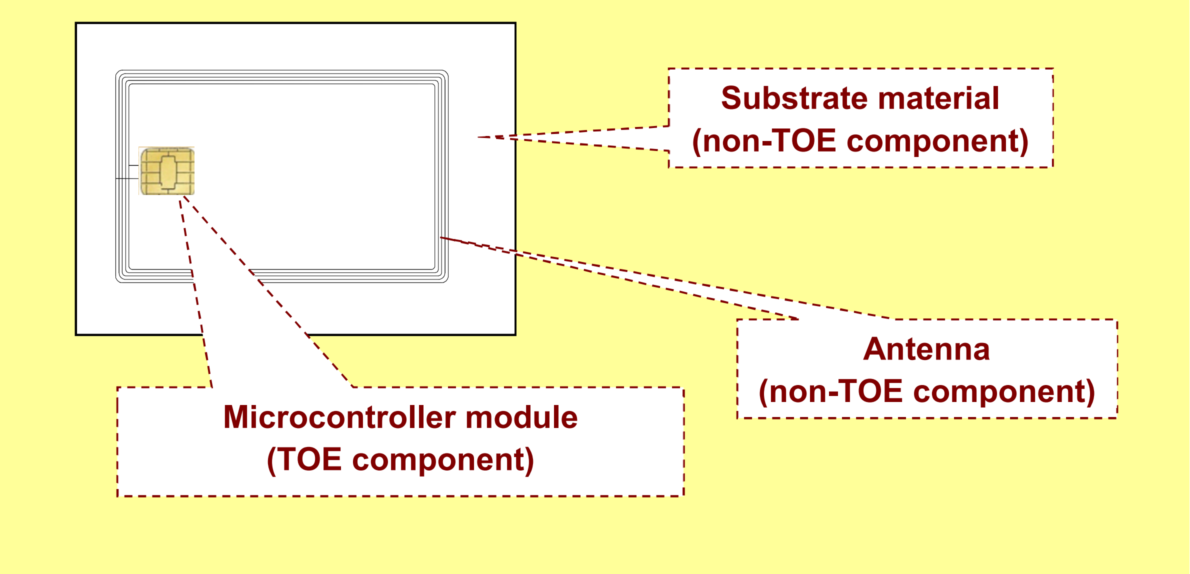
- operating system
- file system
- e-Document applications
- security data objects

The microcontroller family M7892 G12 on which the SOMA-c007 operating system builds is described in Appendix A.
The TOE will be distributed according to the Secure Delivery Procedure [R7].

1.6.2 Other non-TOE physical components

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 SOMA-c007 operating system manages all the resources of the integrated circuit that equips the e-Document, providing secure access to data and functions. Major tasks performed by the operating system are:

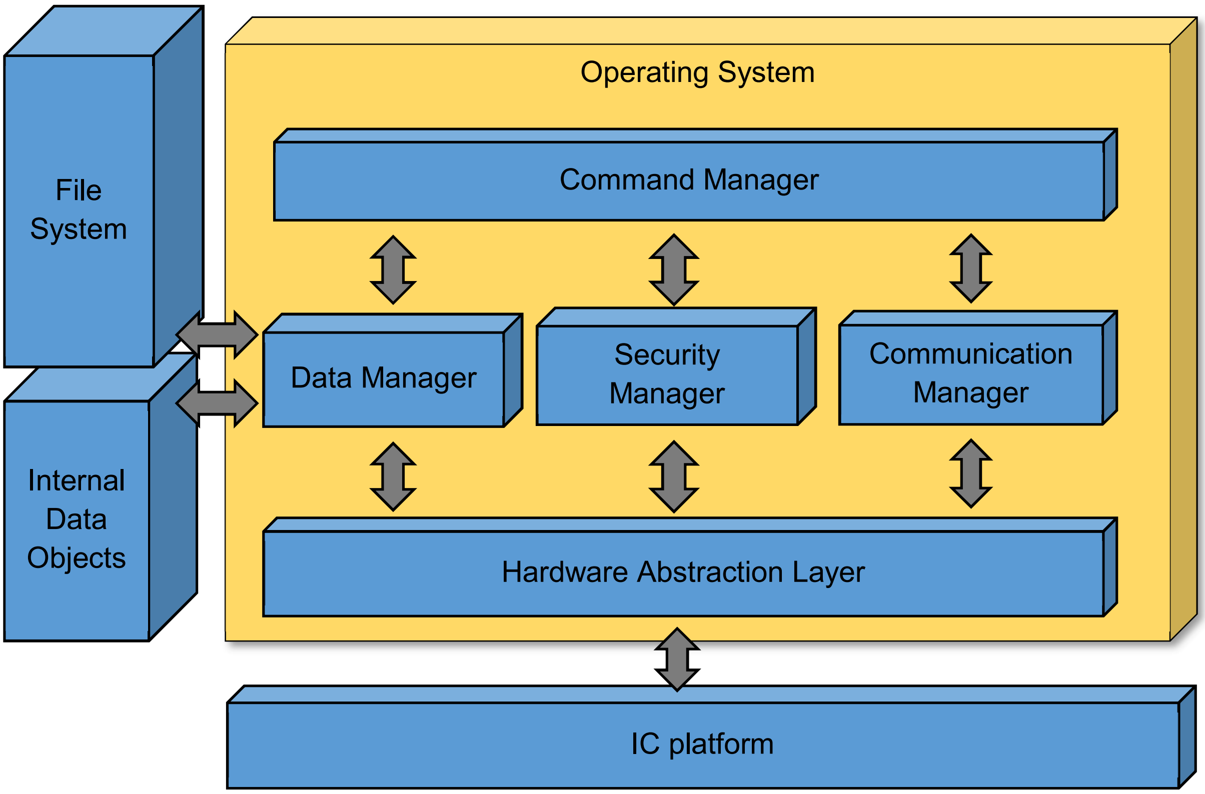
- Communication between internal objects
- Communication with external devices
- Data storage in the file system
- Execution of commands
- Cryptographic operations
- Management of the security policies

Figure 1-3 shows an overview of the TOE architecture. In particular:

- The **Hardware Abstraction Layer** acts as the interface with the IC platform;
- The **Security Manager** provides the cryptographic services (Triple-DES, AES, SHA, MAC), as well as the authentication mechanisms (GIM, CPS, BAC).
- The **Communication Manager** manages both the contact and the contactless communication with the terminal.
- The **Data Manager** provides services for the management of the file system and of data objects, as well as the security status associated with data objects.
- The **Command Manager** provides for the interpretation and execution of commands as well as the management of the security status associated with commands.
- The **File System** holds the LDS application, the data groups and other ISO 7816 dedicated files and elementary files.
- **Internal Data Objects** include the following data:
    - Initialization key,

  - Retry counters,
  - Failure counter,
  - Contact and contactless communication parameters,
  - Memory size information,
  - Life cycle status information,
  - Command enabling bitmask,
  - File system information,
  - Card information.

Figure 1-3 TOE architectural overview



In each life cycle phase/step access to functions and data is restricted by means of cryptographic mechanisms as follows:

- In Step 5 “Initialization” of Phase 2, the Initialization Agent must prove his/her identity by means of an authentication mechanism based on AES with 256-bit key.
- In Step 6 “Pre-personalization” of Phase 2, the Pre-personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In Phase 3 “Personalization”, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on Triple-DES with 112-bit keys.
- In Phase 4 “Operational use”, the user must prove his entitlement to access less sensitive data, i.e. DG1, DG2 and DG5 to DG16, by means of the BAC mechanism compliant to ICAO Doc 9303-11 [R23].

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 [R26].

The integrity of data stored under the LDS is checked by means of the Passive Authentication mechanism defined in [R23]. The BAC and Passive Authentication mechanisms are described in more detail in the following sections.

1.6.3.1 Passive Authentication

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

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

2. The inspection system builds and validates a certification path from a Trust Anchor to the Document Signer Certificate used to sign the Document Security Object (SO_D) according to [R22].

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 [R42], Key Establishment Mechanism 6, using Triple DES [R35] as block cipher. A cryptographic checksum according to [R27], MAC Algorithm 3, is calculated over and appended to the ciphertexts. The modes of operation described in [R23] 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

This Security Target claims conformance to:

- Common Criteria version 3.1 revision 4, International English Version [R16][R17][R18], as follows:
  - Part 2 (security functional requirements) extended
  - Part 3 (security assurance requirements) conformant

The software part of the TOE runs on the chip Infineon *M7892 G12* (Appendix A). This integrated circuit is certified against Common Criteria at the assurance level EAL6+ (cf. [R8]).

2.2 Protection Profile Conformance

This ST 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 25th March, 2009 [R11].

2.3 Package Conformance

This Security Target claims conformance to:

- EAL4 assurance package augmented by ALC_DVS.2 defined in CC part 3 [R18]

2.4 Conformance Rationale

This ST claims strict conformance to the BAC PP [R11]. 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 Seventh Edition 2015. 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 2015.

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 "traveler" 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”, “Initialization Agent” and “Pre-personalization Agent”, acting in Phase 2 “Manufacturing respectively in Step 4 “Card Manufacturing”, Step 5 “Initialization” and Step 6 “Pre-personalization”. Note the Card Manufacturer is a role performing only the physical preparation of the TOE.
In some parts of this ST the Initialization Agent and the Pre-personalization Agent are collectively referred to as “e-Document Manufacturers”.

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

In this ST, the TOE will be delivered from the IC Manufacturer to the Card Manufacturer after Step 3 “IC Manufacturing” of Phase 2, as a chip, in accordance with Application Note 5 of the PP [R11]. At TOE delivery, there is no user data or machine readable data available. The EF.DG14 file, containing part of the user data, is written by the Pre-personalization Agent in Step 6 “Pre-Personalization” of Phase 2. The remaining user data as well as applicative files are written by the Personalization Agent, during Phase 3 “Personalization”.

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

The TOE provides a contact interface according to ISO/IEC 7816-2 [R32]; 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 [R11].

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

Security Objective	Definition	Operation
A.Pers_Agent	Personalization of the MRTD’s chip	The sentence “if stored on the MRTD’s chip” has been removed as EF.DG14 is stored on the chip in Step 6 “Pre-personalization”.
T.Chip_ID	Identification of e-Document’s chip	The definition has been extended to take into account the presence of a contact interface.

Security Objective	Definition	Operation
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 clarify the responsibility of the Issuing state or organization in pre-personalization, and 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 5 Initialization.
OT.AC_Pre-pers	Access control for Pre-personalization of logical e-Document	Added to take into account access control in Step 6 Pre-personalization.
OT.AC_Pers	Access Control for Personalization of logical e-Document.	Modified in a more restrictive way as data addition is not allowed at all after 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). It also states that the IC initialization data include the Initialization key. This Objective now specify that the Initialization Data are split into IC Initialization Data and the TOE Initialization Data, that the IC Initialization Data include the Initialization Key, and that the TOE Initialization Data include the Pre-personalization Keys.
OE.Initialization	Initialization of logical e-Document	Added to take into account responsabilities in Step 5 Initialization
OE.Pre-personalization	Pre-personalization of logical e-Document	Added to take into account responsibilities in Step 6 Pre-personalization

The functional requirements described in section 6 of this ST correspond to the ones in section 5 of the PP [R12].

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 SFRs iterations and refinements

Security Functional Requirement	Operation
FCS_CKM.1/CPS	**Iteration** Iteration that specifies the generation of the session keys for the Pre-personalization Agent and for the Personalization Agent.
FCS_CKM.1/GIM	**Iteration** Iteration that specifies the generation of the Initialization Key.
FCS_CKM.1/BAC	**Iteration** Due to the addition of FCS_CKM.1/CPS and FCS_CKM.1/GIM, an iteration label “BAC” has been added to this SFR to distinguish the generation of the Document BAC keys.
FIA_UAU.5.2	**Refinement** A technical reference to the symmetric authentication mechanism with Personalization keys has been added. The Initialization Agent and the Pre-personalization Agent have been added as users allowed to authenticate to the e-Document. Now this SFR refers the respective authentication mechanisms.
FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers FIA_AFL.1/BAC	**Iteration** Iterations have been added to distinguish between authentication failure handling throughout the TOE life cycle.
FMT_MTD.1/INI_DIS	**Refinement** This SFR has been refined with respect to the PP to indicate that read access to initialization data may be granted by the Pre-personalization Agent only.
FMT_MTD.1/KEY_READ/BAC FMT_MTD.1/KEY_READ/Init FMT_MTD.1/KEY_READ/Pre-pers	**Iteration** Iterations have been added to indicate that read access restriction applies also to the Initialization key and to the Pre-personalization keys. The iteration label “BAC” has been added to the original SFR from the PP to distinguish it from the other iterations.
FMT_SMF.1	**Refinement** The management function “Configuration” has been added.

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 [R22]. 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 as the ICAO Doc 9303 [R23] 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.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, the Initialization Agent and the Pre-personalization 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:
  - IC Manufacturer in Step 3,
  - Card Manufacturer in Step 4,
  - Initialization Agent in Step 5 and
  - Pre-personalization Agent in Step 6.

  The subject Manufacturer collectively identifies the above subjects (see also section 2.4).

- **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 [R22].

- **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 10 *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 11 *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.

- **A.e-Document_Manufact** **e-Document manufacturing on steps 4 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).

- **A.e-Document_Delivery e-Document delivery during steps 4 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.

- **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)
iv. the Document Signer Public Key Certificate (is 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.

- **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 [R23].

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 12 *According to [R23] 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.*

- **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’ [R23], 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 13 *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.

- **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: Anonimity of user

- **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

- **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

- **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 write the digitized portrait and optional biometric reference finger data read from the logical e-Document of a holder into an other MTRD'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

The TOE shall avert the threat as specified below.

- **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

- **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

- **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

- **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 [R16]).

- **P.Manufact** **Manufacturing of the e-Document's chip**

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

- **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.

- **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)[3] 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 [R23].

Application Note 14 *The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [R23]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.*

[3] Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this Protection Profile.

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.

- **OT.AC_Init Access Control for Initialization of logical e-Document**

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

- **OT.AC_Pre-pers Access Control for Pre-personalization of logical e-Document**

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

- **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 [R12] 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 can not be changed after its personalization.

Application Note 15 *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.*

- **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.

- **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 16 *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' [R23] 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.*

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

The TOE must provide means to store IC Identification and other Initialization data, as well as Pre-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 Pre-personalization key(s). The storage of the Pre-Personalization 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 successful authenticated Basic Inspection System.

Application Note 17 *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 to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the e-Document”. The 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. The 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 or as Personalization Agent*.

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

- **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.

- **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 18 *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.*

- **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 high 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.

- **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 19 *A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the 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.

- **OE.e-Document_Manufact Protection of the e-Document Manufacturing**

  Appropriate functionality testing of the TOE shall be used in step 4 to 7.
  During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6 and 7 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

- **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.

- **OE.Initialization Initialization of e-Document**

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

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

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

- **OE.Pre-personalization Pre-personalization of logical e-Document**

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

iii. Create DG14, DG15 and TSF data for the e-Document,

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

- **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

v. establish the correct identity of the holder and create biographical data for the e-Document,

vi. enroll 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

vii. 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.

- **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 [R22].

- **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.

- **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 [R23].

- **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 Objects and the integrity 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.

- **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 Basci 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_Pre-pers	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.Pre-personalization	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	
T.Abuse-Func							x						x	x	x					
T.Information_Leakage								x												
T.Phys-Tamper									x											
T.Malfunction										x										
P.Manufact	x	x				x														
P.Personalization			x			x									x					
P.Personal_Data				x	x															
A.e-Document_Manufact											x		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 the Pre-personalization 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 Initialization Agent equips the TOE with the Pre-personalization key according to **OT.Identification** “Identification and Authentication of the TOE”. The security objective **OT.AC_Pre-pers** limits the management of TSF data and the management of TSF to the Pre-personalization Agent.

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

The OSP **P.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 the e-Document’s chip directly 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 threat **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", **OT.AC_Pre-pers** "Access Control for Pre-personalization 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), Pre-personalization Agent (cf. OE.Pre-personalization) 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", **OE.Pre-personalization** "Pre-personalization of logical e-Document" and **OE.Personalization** "Personalization of logical e-Document" ensuring that the TOE security functions for the initialization, the pre-personalization and the personalization are disabled and the security functions for the operational state after delivery to 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 4 to 6” is covered by the security objectives for the TOE environment **OE.Initialization** “Initialization of the logical e-Document”, **OE.Pre-personalization** “Pre-personalization 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 4 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 objectives 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 ST uses components defined as extensions to CC part 2 [R17]. Some of these components are defined in [R10], other components are defined in the protection profile [R11].

5.1 Definition of the 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 [R11]. 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 behavior:	This family defines functional requirements for the storage of audit data.
Component leveling:	
FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management	There are no management activities foreseen.
Audit	There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the family FCS_RND

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 [R12]. 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

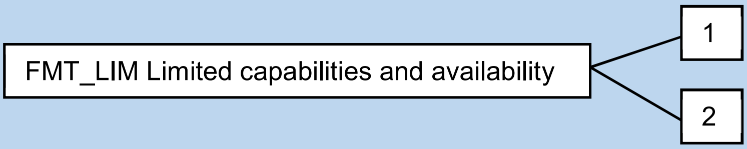
FCS_RND Generation of random numbers	
Family behavior:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component leveling:	
FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components
Dependencies:	No Dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the family 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 behavior:	This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.
Component leveling:	
FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
Management:	There are no management activities foreseen.
Audit:	There are no actions defined to be auditable.

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 20 *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 the family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the PP [R12] to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD 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 [R17].

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

Table 5-4 Family FPT_EMSEC

FPT_EMSEC TOE Emanation	
Family behavior:	This family defines requirements to mitigate intelligible emanations.
Component leveling:	 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 Requirements

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

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

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

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments made by the ST author appear in **underlined bold** text.

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

The definition of the subjects "Manufacturer", "Personalization Agent", "Basic Inspection System" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations "transmit", "receive" and "authenticate" are originally taken from [R17].

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class FAU Security Audit

6.1.1.1 FAU_SAS.1 Audit storage

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (CC part 2).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1	The TSF shall provide the Manufacturer[4] with the capability to store the IC Identification Data[5] in the audit records.

Application Note 21 *The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer, the Initialization Agent and the Pre-personalization Agent in the Manufacturer role write the Initialization Data and Pre-personalization 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).*

6.1.2 Class FCS Cryptographic Support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

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

FCS_CKM.1/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

[4] [assignment: *authorised user*]

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

FCS_CKM.1.1/ BAC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: Document Basic Access Key Derivation Algorithm[6] and specified cryptographic key sizes 112 bit[7], that meet the following: [R23], appendix D.1[8].

Application Note 22 *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 [R23], 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 [R23], section 9.7.4. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.*

FCS_CKM.1/CPS Cryptographic key generation – Generation of CPS session Keys for Pre-personalization and Personalization by the TOE

Hierarchical to: No other components.

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

FCS_CKM.1.1/ CPS	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **CPS Keys Generation Algorithm**[9] and specified cryptographic key sizes **112 bit**[10] that meet the following: **[R19], section 5.2**[11]

Application Note 23 *the TSF allows to generate the session keys for the pre-personalization and personalization processes by the algorithm described in section 5.2 of the EMV CPS specification, [R19], using the keys stored on the chip (the Pre-personalization key in phase 2 and the Personalization keys in phase 3) and a sequence counter provided*

[6] [assignment: *cryptographic key generation algorithm*]

[7] [assignment: *cryptographic key sizes*]

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

[9] [assignment: *cryptographic key generation algorithm*]

[10] [assignment: *cryptographic key sizes*

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

by the IC card to the pre-personalization terminal or to the personalization terminal in response to an INITIALIZE UPDATE command.

FCS_CKM.1/GIM Cryptographic key generation – Generation of the Initialization Key by the TOE

Hierarchical to: No other components.

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

FCS_CKM.1.1/ GIM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Initialization Key Generation Algorithm**[12] and specified cryptographic key sizes **256 bit**[13] that meet the following: **none**[14]

Application Note 24 *the TSF allows to generate the diversified 256-bit AES Initialization key in Step 5 "Initialization" of Phase 2 "Manufacturing" by the algorithm described in the Initialization Guidance [R3], using the key stored on the chip.*

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

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

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]

[12] [assignment: *cryptographic key generation algorithm*]

[13] [assignment: *cryptographic key sizes*

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

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**[15] that meets the following: **none**[16].

Application Note 25 *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.*

6.1.2.3 FCS_COP.1 Cryptographic operation

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

FCS_COP.1/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[17] in accordance with a specified cryptographic algorithm **SHA-1, SHA-256**[18] and cryptographic key sizes none[19] that meet the following: **FIPS 180-2 [R36]**[20].

Application Note 26 *This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [R23], as well as the hash function SHA-256 for the Initialization Agent Authentication Mechanism according to [R3].*

FCS_COP.1/ENC Cryptographic operation –Encryption/Decryption Triple DES

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

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

[17] [assignment: *list of cryptographic operations*]

[18] [selection: *SHA-1, SHA-224, SHA-256 or other approved algorithms*]

[19] [assignment: *cryptographic key sizes*]

[20] [selection: *FIPS 180-2 or other approved standards*]

Hierarchical to: No other components.

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

FCS_COP.1.1/ ENC	The TSF shall perform secure messaging – encryption and decryption[21] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[22] and cryptographic key sizes 112 bit[23] that meet the following: FIPS 46-3 [R35] and [R23] section 9.8[24].

Application Note 27 *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.*

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

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]

FCS_COP.1.1/AUTH	The TSF shall perform symmetric authentication – encryption and decryption[25] in accordance with a specified cryptographic algorithm **Triple-DES and AES**[26] and cryptographic key sizes: **112 bit for Triple-DES and 256 bit for AES**[27] that meet the following: **FIPS 46-3 and FIPS 197**[28]

Application Note 28 *This SFR requires the TOE to implement the cryptographic primitive AES in CBC mode for authentication attempt of a terminal as Initialization Agent in Step 5: Initialization of Phase 2: Manufacturing, according to the Initialization Guidance [R3].*

Application Note 29 *This SFR requires the TOE to implement the cryptographic primitive Triple-DES for authentication attempt of a terminal as Pre-personalization Agent or as Personalization Agent by means of the CPS mechanism (cf. FIA_UAU.4).*

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[29] in accordance with a specified cryptographic algorithm Retail MAC[30] and cryptographic key sizes 112 bit[31] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [R27][32].

Application Note 30 *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted*

[25] [assignment: *list of cryptographic operations*]
[26] [selection: *Triple-DES, AES*]
[27] [selection: 112, 128, 168, 19, 256]
[28] [selection: FIPS 46-3, FIPS 197]
[29] [assignment: *list of cryptographic operations*]
[30] [assignment: *cryptographic algorithm*]
[31] [assignment: *cryptographic key sizes*]
[32] [assignment: listo f standards]

data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1and FIA_UAU.4.

6.1.2.4 FCS_RND.1 Quality metrics for random numbers

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

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **BSI AIS-31 functionality class PTG.2 [R9] (see Application Note 32)** [33].

Application Note 31 *This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.*

Application Note 32 *The TOE makes use of the true random number generator (TRNG) of the IC M7892 G12. The TRNG has already been evaluated as conformant to class PTG.2 of BSI-AIS31 with strength of mechanism: high.*

6.1.3 Class FIA Identification and Authentication

Application Note 33 *Table 6-1 provides an overview on the authentication mechanisms*

Table 6-1 Overview of the authentication mechanisms used

Mechanism	SFR for the TOE	Algorithms and key sizes according to [R23] and [R14]
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)
Authentication Mechanism for Initialization Agent	FIA_UAU.4 FIA_AFL.1/Init	AES with 256-bit key (cf. FCS_COP.1/AUTH)

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

CPS mechanism for Pre-personalization Agent	FIA_UAU.4 FIA_AFL.1/Pre-pers	Triple-DES with 112 bit keys (cf. FCS_COP.1/AUTH)
CPS Authentication Mechanism for Personalization Agent	FIA_UAU.4 FIA_AFL.1/Pers	Triple-DES with 112 bit keys (cf. FCS_COP.1/AUTH)

6.1.3.1 FIA_UID.1 Timing of identification

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1	The TSF shall allow: 1. to read the IC Initialization Data in Phase 2 "Manufacturing", 2. to read the random identifier in Phase 3 "Personalization of the e-Document", 3. to read the random identifier in Phase 4 "Operational Use"[34] 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 34 *In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role available for the TOE. The Pre-personalization Agent may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the e-Document". 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.*

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

Application Note 35 *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.*

6.1.3.2 FIA_UAU.1 Timing of authentication

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria part 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: 1. to read the IC Initialization data in Phase 2 "Manufacturing", 2. to read the random identifier in Phase 3 "Personalization of the e-Document", 3. to read the random identifier in Phase 4 "Operational Use"[35]. 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 36 *The Basic Inspection System and the Personalization Agent authenticate themselves.*

6.1.3.3 FIA_UAU.4 Single-use authentication mechanisms

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

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1. Basic Access Control Authentication Mechanism, 2. Authentication Mechanism based on **Triple-DES and AES**[36].

Application Note 37 *The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [6]. 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 fulfill the security objective OT.Identification and to prevent T.Chip_ID.*

6.1.3.4 FIA_UAU.5 Multiple authentication mechanisms

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

[36] [selecion: *Triple-DES, AES or another approved algorithms*]

FIA_UAU.5.1	The TSF shall provide 1. Basic Access Control Authentication Mechanism, 2. Symmetric authentication mechanism based on **Triple-DES [R19] and AES [R3]**[37] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: 1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms: **the Symmetric Authentication Mechanism with Personalization keys**, **Refinement: according to [R19]** 2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys[38] **Refinement:** **3. the TOE accepts the authentication attempt as Initialization Agent by the following mechanisms: Symmetric Authentication Mechanism based on AES with Initialization key, according to [R3],** **4. the TOE accepts the authentication attempt as Pre-personalization Agent by the following mechanisms: the CPS Mechanism with Pre-personalization keys, according to [R19],**

Application Note 38 *The Symmetric Authentication Mechanism for the Initialization Agent is based on AES with 256-bit key as described in [R3].*

Application Note 39 *The Symmetric Authentication Mechanism for the Pre-personalization Agent and Personalization Agent is based on the CPS protocol* [R19] *based on Triple-DES. This mechanism uses a key diversification algorithm based on data randomly chosen by the card. Note that Application Note 31 in the BAC PP [R11] is subordinated to the compliance with the EAC PP. However, the formulation of FIA_UAU.5 in both the EAC PP [R12] and the PACE PP [R13], to which the EAC ST [R1] claims compliance, does not forbid the use of Triple-DES for the agent authentication in the manufacturing phase.*

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

[38] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Application Note 40 *The authentication mechanisms for the Pre-personalization Agent and 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 inspection system.*

6.1.3.5 FIA_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE

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

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[39].

Application Note 41 *The Basic Access Control Mechanism specified in [R23] 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 42 *Note that in case the TOE should also fulfil [R12] 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.*

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

6.1.3.6 FIA_AFL.1 Authentication failure handling

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (CC part 2).

FIA_AFL.1/Init Authentication failure handling in Step 5 "Initialization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Init	The TSF shall detect when **31**[40] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the Initialization key**[41].
FIA_AFL.1.2/Init	When the defined number of consecutive unsuccessful authentication attempts has been **met**[42], the TSF shall **block the Initialization key**[43].

FIA_AFL.1/Pre-pers Authentication failure handling in Step 6 "Pre-personalization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Pre-pers	The TSF shall detect when **3**[44] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the Pre-personalization key**[45].

[40] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[41] [assignment: list of authentication events]

[42] [assignment: *met or surpassed*]

[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/Pre-pers	When the defined number of consecutive unsuccessful authentication attempts has been **met**[46], the TSF shall **block the Pre-personalization key**[47].

FIA_AFL.1/Pers Authentication failure handling in Step 7 "Personalization"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/Pers	The TSF shall detect when **an administrator configurable positive integer within the range between 1 and 15**[48] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the Personalization key**[49].
FIA_AFL.1.2/Pers	When the defined number of consecutive unsuccessful authentication attempts has been **met**[50], the TSF shall **block the Personalization key**[51].

FIA_AFL.1/BAC Authentication failure handling in Step 8 "Operational Use"

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

[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*]

FIA_AFL.1.1/BAC	The TSF shall detect when **an administrator configurable positive integer within the range between 1 and 255**[52] unsuccessful authentication attempts occur related to **consecutive failed authentication attempts with respect to the BAC key**[53].
FIA_AFL.1.2/BAC	When the defined number of consecutive unsuccessful authentication attempts has been **met**[54], the TSF shall **issue the result of the authentication with a few seconds delay**[55].

Application Note 43 *The count of consecutive unsuccessful authentications is stored in non-volatile memory and is preserved across power-up and power-down cycles. After a successful authentication the count is reset to zero.*

6.1.4 Class FDP User Data Protection

6.1.4.1 FDP_ACC.1 Subset access control

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

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1	The TSF shall enforce the Basic Access Control SFP[56] 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[57].

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

[52] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[53] [assignment: list of authentication events]

[54] [assignment: *met or surpassed*]

[55] [assignment: *list of actions*]

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

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

6.1.4.2 FDP_ACF.1 Basic Security attribute based access control

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

FDP_ACF.1 Basic Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1	The TSF shall enforce the Basic Access Control SFP[58] to objects based on the following: 1. Subjects: a. Personalization Agent, b. Basic Inspection System, c. Terminal. 2. Objects: a. data EF.DG1 to EF.DG16 of the logical e-Document, b. data in EF.COM, c. data in EF.SOD. 3. Security attributes: a. authentication status of terminals[59]. -

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

[59] [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*]

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical e-Document, 2. the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical e-Document[60].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[61].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rule: 1. Any Terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical e-Document 2. Any Terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical e-Document 3. The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4[62]

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.* [R1] *for details).*

Application Note 46 *The read access to user data in the personalization phase is protected by a Restricted Application Secret Code.*

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

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

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

Application Note 47 *Access to EF.DG.15 is not listed in FDP_ACF.1 because this ST does not address Active Authentication.*

Inter-TSF-Transfer

Application Note 48 *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.*

6.1.4.3 FDP_UCT.1 Basic data exchange confidentiality

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

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[63] to be able to transmit and receive[64] user data in a manner protected from unauthorized disclosure.

6.1.4.4 FDP_UIT.1 Data exchange integrity

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

FDP_UIT.1 Data exchange integrity - e-Document

Hierarchical to: No other components.

[63] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[64] [selection: *transmit, receive*]

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[65] to be able to transmit and receive[66] user data in a manner protected from modification, deletion, insertion and replay[67] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[68] has occurred.

6.1.5 Class FMT Security Management

Application Note 49 *The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.*

6.1.5.1 FMT_SMF.1 Specification of Management Functions

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

[65] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[66] [selection: *transmit, receive*]
[67] [selection: *modification, deletion, insertion, replay*]
[68] [selection: *modification, deletion, insertion, replay*]

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Initialization, 2. Pre-Personalization, 3. Personalization, **Refinement:** 4. **Configuration.**[69]

Application Note 50 *The ability to initialize, personalize and configure the TOE is restricted to a successfully authenticated Initialization Agent or Pre-personalization Agent or Personalization Agent by means of symmetric keys. Initialization keys are only active on uninitialized products. Pre-personalization Keys are only active in products already initialized but not pre-personalized yet. Personalization keys are only active in pre-personalized but not personalized products. The e-Document locks out after a programmable number of consecutive unsuccessful authentication attempts. After the completion of the initialization, the Initialization key is no longer usable. The Pre-personalization Keys are disabled once pre-personalization is complete.*

6.1.5.2 FMT_SMR.1 Security roles

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (CC part 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: 1. Manufacturer, 2. Personalization Agent, 3. Basic Inspection System [70].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

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

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

Application Note 51 *The role Manufacturer collectively refers to the IC Manufacturer, the Initialization Agent and the Pre-personalization Agent.*

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.

6.1.5.3 FMT_LIM.1 Limited capabilities

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow: 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks.

6.1.5.4 FMT_LIM.2 Limited availability

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow: 1. User Data to be disclosed or manipulated, 2. TSF data to be disclosed or manipulated, 3. software to be reconstructed and 4. substantial information about construction of TSF to be gathered which may enable other attacks.

Application Note 52 *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.

6.1.5.5 FMT_MTD.1 Management of TSF data

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

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and 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[71] the Initialization Data and Pre-personalization Data[72] to the Manufacturer[73].

[71] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[72] [assignment: *list of TSF data*]

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

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

Application Note 54 *the pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent, which is the symmetric cryptographic Personalization Agent Authentication Key.*

Application Note 55 *IC Initialization Data are written by the IC Manufacturer in Step 3, TOE Initialization Data are written by the Initialization Agent in Step 5 and Pre-personalization Data are written by the Pre-personalization Agent in Step 6, according to the life cycle description given in section 1.5.*

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	The TSF shall restrict the ability to disable read access for users to[74] the Initialization Data[75] to **Refinement:** **the Pre-personalization Agent**[76].

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

[74] [selection: *change_default, query, modify, dolete, clear, [assignment: other operations]*]

[75] [assignment: *list of TSF data*]

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

FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_WRITE	The TSF shall restrict the ability to write[77] the Document Basic Access Keys[78] to the Personalization Agent[79].

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[80] the Document Basic Access Keys and the Personalization keys[81] to none[82].

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[83] **the Initialization Key** [84] to none[85].

FMT_MTD.1/KEY_READ/Pre-pers Management of TSF data – Pre-personalization Keys Read

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ KEY_READ/Pre-pers	The TSF shall restrict the ability to read[86] **the Pre-personalization Keys** [87] to none[88].

Application Note 56 *The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.*

6.1.6 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.

6.1.6.1 FPT_EMSEC.1 TOE emanation

The TOE shall meet the requirement "TOE emanation (FPT_EMSEC.1)" as specified below (CC part 2 extended):

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

[86] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[87] [assignment: *list of TSF data*]

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

FPT_EMSEC.1.1	The TOE shall not emit **electromagnetic and current emissions**[89] in excess of **intelligible threshold**[90] enabling access to Personalization key[91] and **Initialization key, Pre-personalization Key**[92]
FPT_EMSEC.1.2	The TSF shall ensure any unauthorized users[93] are unable to use the following interface smart card circuits contacts[94] to gain access to Personalization keys[95] and **Initialization key, Pre-personalization keys**[96]

Application Note 57 *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.*

6.1.6.2 FPT_FLS Failure with preservation of secure state

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).

FPT_FLS.1 Failure with preservation of secure state

[89] [assignment: *type of emissions*]
[90] [assignment: *specified limits*]
[91] [assignment: *list of types of TSF data*]
[92] [assignment: *list of types of user data*]
[93] [assignment: *type of users*]
[94] [assignment: *type of connection*]
[95] [assignment: *list of types of TSF data*]
[96] [assignment: *list of types of user data*]

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. exposure to operating conditions where therefore a malfunction could occur, 2. failure detected by TSF according to FPT_TST.1[97]

6.1.6.3 FPT_TST.1 TSF testing

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria part 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**[98] **, and at the conditions: before any use of TSF data**[99] to demonstrate the correct operation of the TSF[100].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[101].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application Note 58 *A dedicated software in the protected ROM of the IC M7892 G12 provides full test capabilities (operating system for test, "OST"), not accessible by the Security IC Embedded Software after delivery.*

Application Note 59 *At start-up the OS checks whether a reset has been triggered by a sensor. If this is the case, a reset counter is incremented. If the count exceeds 32, then the*

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

[98] [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]*]

[99] *[assignment: conditions under which self test should occur]*]

[100] [selection: *[assignment: parts of TSF], the TSF*]

[101] [selection: *[assignment: parts of TSF], TSF data*]

chip is irreversibly blocked. Before any read of the TSF data, the EEPROM memory is checked for possible fault injection events. If this is the case, the reset counter is incremented and the chip goes into an endless loop. During normal operation, tests of the random number generation and integrity checks are also executed.

Application Note 60 *FPT_TST.1.3 protects the integrity of the code by physical means, using the mechanisms of the underlying IC. After delivery, the TOE does not use logical means to check the integrity of the code, as it relies on the IC security features to provide verification of the code integrity.*

6.1.6.4 FPT_PHP.3 Resistance to physical attack

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[102] to the TSF[103] by responding automatically such that the SFRs are always enforced.

Application Note 61 *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 response" means here:*

- *assuming that there might be an attack at any time and*
- *countermeasures are provided at any time.*

6.2 Security Assurance Requirements for the TOE

The components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the component ALC_DVS.2.

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

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

Table 6-2 summarizes the assurance components that define the security assurance requirements for the TOE.

Table 6-2 Assurance requirements at EAL4+

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

6.3 Security Requirements Rationale

6.3.1 Security functional requirements rationale

Table 6-3 provides an overview for security functional requirements coverage of security objectives.

Table 6-3 Coverage of Security Objectives for the TOE by SFR

	OT.AC_Init	OT.AC_Pre-pers	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/CPS		X	X	X						
FCS_CKM.1/GIM	X			X						
FCS_CKM.4	X	X	X		X					
FCS_COP.1/SHA		X	X	X	X					
FCS_COP.1/ENC	X	X	X	X	X					
FCS_COP.1/AUTH		X	X	X						
FCS_COP.1/MAC	X	X	X	X	X					
FCS_RND.1		X	X	X	X					
FIA_UID.1					X	X				

	OT.AC_Init	OT.AC_Pre-pers	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
FIA_AFL.1/Init						X				
FIA_AFL.1/Pre-pers						X				
FIA_AFL.1/Pers						X				
FIA_AFL.1/BAC					X	X				
FIA_UAU.1					X	X				
FIA_UAU.4	X	X	X	X	X					
FIA_UAU.5	X	X	X	X	X					
FIA_UAU.6			X	X	X					
FDP_ACC.1	X	X	X	X	X					
FDP_ACF.1	X	X	X	X	X					
FDP_UCT.1				X	X					
FDP_UIT.1				X	X					
FMT_SMF.1	X	X	X	X	X					
FMT_SMR.1	X	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									
FMT_MTD.1/KEY_READ/Pre-pers		X								
FPT_EMSEC.1	X	X	X				X			
FPT_TST.1							X		X	
FPT_FLS.1	X	X	X				X		X	
FPT_PHP.3	X	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 5 “Initialization”. The write access to the logical e-Document data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Initialization Agent is allowed to write the OS configuration data of the logical e-Document only once.

The authentication of the terminal as Initialization Agent shall be performed by TSF according to SRF 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 (FCS_CKM.1/GIM).

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 ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.AC_Pre-pers** “Access Control for Pre-personalization of logical e-Document” addresses the access control of the writing the logical e-Document in Step 6 “Pre-personalization”. The write access to the logical e-Document data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Pre-personalization Agent is allowed to write the data groups EF.DG14 and EF.DG15 of the logical e-Document only once.
The authentication of the terminal as Pre-personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Pre-personalization Agent is authenticated by using the CPS mechanism based on Triple-DES (FCS_CKM.1/CPS, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the Pre-personalization keys by using the CPS mechanism (FCS_COP.1/AUTH).
The SFR FMT_SMR.1 lists the roles (including Pre-personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Pre-personalization). The SFR FMT_MTD.1/KEY_READ/Pre-pers prevents read access to the secret key of the Pre-personalization Agent and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys. The SFR FCS_CKM.1/CPS allows to protect the transmitted data by means secure messaging during the pre-personalization process.

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 SFR 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.DG13, EF.DG16 of the logical e-Document only once.
The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated by using the CPS mechanism based on Triple-DES (FCS_CKM.1/CPS, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key by using the CPS mechanism (FCS_COP.1/AUTH).

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 keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The SFR FCS_CKM.1/CPS allows to protect the transmitted data by means secure messaging during the initialization and personalization processes.

Application Note 62 *The TOE does not allow 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 SFR
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 SRF 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 SFR 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, FCS_COP.1/SHA, FCS_RND.1 (for key generation), FCS_CKM.1/GIM (for the generation of the Initialization Key), FCS_CKM.1/CPS (for the generation of the personalization keys) and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_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 SFR 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 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 the 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 ENC_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), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, 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” address 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 and Pre-personalization 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 SFR 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 37). In case of failed authentication attempts FIA_AFL.1/Init, FIA_AFL.1/Pre-pers, FIA_AFL.1/Pers block the authentication key, 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 SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

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

The security objective **OT.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,
ii. the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2 Dependency Rationale

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

Table 6-4 shows the dependencies between the SFR of the TOE.

Table 6-4 Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
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 and FCS_COP.1/MAC Fulfilled by FCS_CKM.4,
FCS_CKM.1/CPS	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ENC, FCS_COP.1/MAC Fulfilled by FCS_CKM.4,
FCS_CKM.1/GIM	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/SHA 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, FCS_CKM.1/CPS and FCS_CKM.1/GIM.

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.1Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Justification 1 for non-satisfied dependencies Fulfilled by FCS_CMK.4
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/CPS and FCS_CKM.1/GIM. 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 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 and FCS_CKM.1/CPS. Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.
FIA_UAU.6	No dependencies	n.a.
FIA_AFL.1/Init	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/Pre-pers	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 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	n.a.
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
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_READ/Pre-pers	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	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Justifications for non-satisfied dependencies between the SFR 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 uses the symmetric Initialization Key, Pre-personalization Key and Personalization Key permanently stored, respectively, during the IC Manufacturing, Initialization and Pre-personalization processes (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1 or FDP_ITC. Since the key is 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 the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

Justification 4: The SFR FDP_UCT.1 and FDP_UIT.1 require the use 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.

6.3.3 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 augmented to EAL4 has no dependencies to other security requirements.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

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

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

- The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, 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 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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

7. TOE Summary Specification

The following sections provide a general understanding of how the TOE is implemented. To facilitate reading, the description of the security features of the TOE is organized in security services. A requirements traceability matrix against each security service is given in Table 7-2.

7.1 Coverage of SFRs

7.1.1 SS.AG_ID_AUTH Agents Identification & Authentication

This security service meets the following SFRs:
FCS_CKM.1/GIM, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FCS_COP.1/AUTH, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_AFL.1/Init, FIA_AFL.1/Pre-pers, FIA_AFL.1/Pers, FIA_AFL.1/BAC.

Access to functions and data of the TOE is only allowed to authenticated users. The authentication mechanism applied depends on the system used for operations. Table 7-1 summarizes the authentication mechanisms for the various systems, later detailed in this section.

Table 7-1 Summary of authentication mechanisms

System type	e-Document Life-Cycle status	Authentication Mechanism
Initialization system	Non-initialized	Decryption of initialization cryptograms based on AES with 256-bit Initialization key, as described in [R3].
Pre-personalization system	Non-Initialized	CPS authentication based on Triple-DES with 112-bit Pre-personalization Keys
Personalization System	Initialized	CPS authentication based on Triple-DES with 112-bit Personalization keys
Basic Inspection System	Operational	BAC based on Triple-DES with 112-bit Document Basic Access Keys

The Initialization Agent authenticates to the e-Document by decrypting the initialization cryptograms (FCS_CKM.1/GIM, FCS_COP.1/AUTH) using the algorithm described in [R3] based on AES in CBC mode with 256-bit key. The Initialization Agent has a limited number of authentication attempts after which the Initialization Agent authentication mechanism is disabled (FIA_AFL.1/Init).

The Pre-personalization Agent and the Personalization Agent authenticate themselves to the e-Document by means of a mutual authentication mechanism based on the protocol defined in EMV CPS specification, section 4.1, 5.2. [R19] (FIA_UID.1, FIA_UAU.1, FIA_UAU.5). The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5) (FCS_COP.1/ENC) and the message authentication code computation accords to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/MAC).
This function detects each unsuccessful authentication attempt. The Pre-personalization Agent and the Personalization Agent have only a limited number of authentication attempts after which the related keys are blocked.
In case of regular termination of the protocol, both parties possess authentic keying materials only known to them. The user may establish a secure messaging session (FCS_CKM.1/CPS) and at the end of the session, the session keys are securely erased (FCS_CKM.4).

The Basic Access System and the e-Document mutually authenticate by means of a Basic Access Control mechanism based on a three pass challenge-response protocol (FIA_UID.1, FIA_UAU.1, FIA_UAU.5). The challenge is the random number sent from one party to the other. This random number will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. This security service manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303 [R23]) (FCS_COP.1/ENC), while the message authentication code is computed according to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) (FCS_COP.1/MAC). These authentication keys are derived by the SHA-1 algorithm (FIPS 180-2) as described in the ICAO Doc 9303 [R23] (FCS_COP.1/SHA).
After a successful BAC authentication, the Basic Access System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources.

In the operational use phase, the TOE identification data can be obtained by an authenticated BIS only. A BAC-like mechanism is used for this authentication (FIA_UAU.5).

7.1.2 SS.SEC_MSG Data exchange with Secure Messaging

This security service meets the following SFRs:
FCS_CKM.1/BAC, FCS_CKM.1/CPS, FCS_COP.1/SHA, FCS_CKM.1/ENC, FCS_CKM.4, FCS_COP.1/MAC, FCS_COP.1/AUTH, FIA_UAU.6.

This security service concerns the creation and the management of a secure communication channel for the sensitive data exchange between the TOE and the Inspection System. On this channel the data will be encrypted and authenticated with session keys (data Triple-DES-encryption and MAC computation) such that the TOE is able to verify the integrity and authenticity of received data. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303, normative appendix 5), while the message authentication code is according to Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). The session keys are calculated during the authentication phase. The secure messaging channel will be closed in case of a received message with:

- inconsistent or missing MAC,
- wrong sequence counter,
- plain access.

Session keys are overwritten after usage (FCS_CKM.4).

7.1.3 SS.ACC_CNTRL Access Control of stored Data Objects

This security service meets the following SFRs:
FAU_SAS.1, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ/BAC, FMT_MTD.1/KEY_READ/Init, FMT_MTD.1/KEY_READ/Pre-pers.

As required in FDP_ACF.1, read and write access to stored data must be controlled in different phases of the production and during operational use.
This security service ensures that the assets (user data and TSF data) can only be accessed as defined by the access right written during the personalization process and allows the access to the TOE identification data in the Personalization phase. Furthermore, the access conditions allow to differentiate the roles based on the knowledge of secret keys. Any access not explicitly allowed is denied.

The Document Basic Access Keys, the Document Number and the Security Environment object will be written during the personalization phase by the Personalization Agent.

After keys have been written any type of direct access to any key is not allowed (FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ/BAC, FMT_MTD.1/KEY_READ/Init, FMT_MTD.1/KEY_READ/Pre-pers).

7.1.4 SS.LFC_MNG Life cycle management

This security service meets the following SFRs:

FMT_SMF.1, FMT_SMR.1

It ensures that the TOE life cycle status is set in an irreversible way to mark the following phases in the given order: manufacturing, personalization and operational use. The only role allowed to set the life cycle status is the Manufacturer.
The transition between the manufacturing phase and personalization phase is performed disabling the Pre-personalization Keys.

7.1.5 SS.SW_INT_CHECK Software integrity check of TOE's assets

This security service meets the following SFRs:
FMT_LIM.1, FMT_LIM.2, FPT_TST.1

The TOE doesn't allow to analyze, debug or modify TOE's software during the operational use. In phase 3 and 4 no commands are allowed to load executable code. Self tests will be executed at initial start-up on ROM area (this functionality is implemented by the underlying hardware).
This security service also checks the integrity of the following assets:

- application files,
- security data objects.

Integrity checks will be executed before any use of TSF data.
This SF warns the entity connected upon detection of an integrity error of the sensitive data stored within the TOE Scope of Control and preserves a secure state when failure is detected by TSF.

7.1.6 SS.SF_HW Security features provided by the hardware

This security service meets the following SFRs: FCS_RND.1, FMT_LIM.1, FMT_LIM.2, FPT_EMSEC.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.3.

The TOE benefits of a set of features provided by the integrated circuit to enforce security. The security features of the hardware platform are reported in [R25]. These security functions have already been evaluated and certified being the chips already certified; a more detailed formulation of the security functions provided by the chip can be found in the related security target [R25].

Table 7-2 shows the coverage of SFR by the security services described above.

Table 7-2 Coverage of SFRs by security services

	SS.AG_ID_AUTH Agents Identification & Authentication	**SS.SEC_MSG** Data exchange with Secure Messaging	**SS.ACC_CNTRL** Access Control of Stored Data Object	**SS.LFC_MNG** Life Cycle Management	**SS.SW_INT_CHECK** SW Integrity check of TOE's Assets	**SS.SF_HW** Security features provided by the hardware
FAU_SAS.1			X			
FCS_CKM.1/BAC		X				
FCS_CKM.1/CPS		X				
FCS_CKM.1/GIM	X					
FCS_CKM.4	X	X				
FCS_COP.1/SHA		X				
FCS_COP.1/ENC		X				
FCS_COP.1/AUTH	X	X				
FCS_COP.1/MAC		X				
FCS_RND.1						X
FIA_UID.1	X					
FIA_UAU.1	X					
FIA_UAU.4	X					
FIA_UAU.5	X					
FIA_UAU.6		X				
FIA_AFL.1/Init	X					
FIA_AFL.1/Pre-perso	X					
FIA_AFL.1/Perso	X					
FIA_AFL.1/BAC	X					
FDP_ACC.1			X			
FDP_ACF.1			X			
FDP_UCT.1			X			
FDP_UIT.1			X			
FMT_SMF.1			X	X		
FMT_SMR.1			X	X		
FMT_LIM.1			X		X	X
FMT_LIM.2			X		X	X
FMT_MTD.1/INI_ENA			X			
FMT_MTD.1/INI_DIS			X			
FMT_MTD.1/KEY_WRITE			X			
FMT_MTD.1/KEY_READ/BAC			X			
FMT_MTD.1/KEY_READ/Init			X			
FMT_MTD.1/KEY_READ/Pre-pers			X			
FPT_EMSEC.1						X
FPT_TST.1					X	X
FPT_FLS.1						X
FPT_PHP.3						X

7.2 Assurance Measures

Assurance measures applied to the TOE are fully compliant to those described in part 3 of the Common Criteria v3.1 [R18].

The implementation is based on a description of the security architecture of the TOE and on 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 pre-personalization 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 a dedicated document 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) will be covered in documents from the IC manufacturer. Security procedures described in such documents have been taken into consideration.

Table 7-3 shows the documentation that provides the necessary information related to the assurance requirements defined in this security target.

Table 7-3 Assurance Requirements documentation

Security Assurance Requirements	Documents
ADV_ARC.1	Description of the Security Architecture of the SOMA-c007 embedded software
ADV_FSP.4	Functional Specification for the SOMA-c007 embedded software
ADV_IMP.1	Source code of the SOMA-c007 embedded software
ADV_TDS.3	Description of the Design of the SOMA-c007 embedded software
AGD_OPE.1	Personalization Guidance for the SOMA-c007 electronic document User Guidance for the SOMA-c007 electronic document
AGD_PRE.1	Pre-personalization guidance for the SOMA-c007 electronic document.
ALC_CMC.4, ALC_CMS.4	Configuration Management Plan, configuration list evidences of configuration management
ALC_DEL.1	Secure Delivery procedure Delivery documentation
ALC_DVS.2	Development security description Development security documentation
ALC_LCD.1	Life-cycle definition
ALC_TAT.1	Tools and techniques definition
ATE_COV.2	Coverage of Test Analysis for the SOMA-c007 Electronic document
ATE_DPT.1	Depth of Test Analysis for the SOMA-c007 Electronic document

Security Assurance Requirements	Documents
ATE_FUN.1	Functional Test Specification for the SOMA-c007 Electronic document Evidences of tests
ATE_IND.2	Documentation related to an independent test.
AVA_VAN.3	Documentation related to an independent vulnerability analysis.

Assurance measures described in this section cover the assurance requirements in section 6.3.3.

8. References

8.1 Acronyms

BAC	Basic Access Control
BIS	Basic Inspection System
C_{DS}	DS Public Key Certificate
CBC	Cipher-block Chaining (block cipher mode of operation)
CC	Common Criteria
COM	Common data group of the LDS (ICAO Doc 9303)
CPS	Common Personalization System
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO Doc 9303)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
ESW	Embedded Software
GIM	Generic Initialization Mechanism
GIS	General Inspection System
IC	Integrated Circuit
IS	Inspection System
LDS	Logical Data Structure
LCS	Life Cycle Status
MAC	Message Authentication Code
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRZ	Machine Readable Zone
N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SO$_D$	Document Security Object
SOF	Strength of Function
SPA	Simple Power Analysis
ST	Security Target
TDES	Triple-DES
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TR	Technical Report
VIZ	Visual Inspection Zone

8.2 Glossary

Active Authentication	Security mechanism defined in ICAO Doc 9303 [R23] option 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-Documents chip to store the Initialization Data and Pre-personalization Data.
authenticity	Ability to confirm the e-Document and its data elements on the e-Document's chip were created by the Issuing State or Organization.
Basic Access Control	Security mechanism defined by ICAO [R23] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with the Document BAC Keys.
Basic Inspection System	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 Readble Zone (MRZ) on the biographical data of an e-Document [R22].
biometric reference data	Data stored for biometric authentication of the e-Document holder in the e-Document's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level . The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Chip Authentication	Authentication protocol used to verify the genuinity of the e-Document chip.
counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Country Signing Certification Authority (CSCA)	Certification Authority of the Issuing State or Organization which attests the validity of certificates and digital signatures issued by the Document Signer.
Country Signing Certification Authority Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (PK_{CSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority (CVCA)	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the e-Document.
Current Date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new keys is before the certificate expiration date of the certificate for the old key.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption and message authentication of data transmitted between the e-Document's chip and

	the inspection system [R23]. It is derived from the printed MRZ of the e-Document book or card to authenticate an entity able to read the printed MRZ of the e-Document book or card.
Document Security Object	A RFC3369 CMS Signed Data Structure, signed by the Document Signer. It carries the hash values of the LDS DG's and is stored in the e-Document's chip. It may carry the Document Signer Certificate (C_{DS}) [R22].
Document Signer	Entity delegated by the Issuing State or Organization to digitally sign the DG's present in the LDS.
eavesdropper	A threat agent with low 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.
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 [R22], ii. the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG 16) and iii. the TSF Data including the definition the authentication data but except the authentication data itself.
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	An integrated circuit chip complying with ISO/IEC 14443 and programmed according to the LDS [R22].
e-Document's chip Embedded Software	Software embedded in a e-Document's chip and not being developed by the IC Designer. The e-Document's chip Embedded Software is designed in phase 1 and embedded into the e-Document's chip in Phase 2 of the TOE life-cycle.

enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [R22].
Extended Access Control	Security mechanism identified in BSI TR-03110 [R14][R15] by which means the MTRD'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. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Keys and to get write and read access to the logical e-Document and TSF data.
Extended Inspection System	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 terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [R22].
General Inspection System	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 Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits 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.

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 Integrated Circuits Manufacturer or by the Initialization Agent (Phase 2). These data are, for instance, used for OS configuration, for traceability and for IC identification as e-Document's material (IC identification data).
inspection	The act of a State examining an e-Document presented to it by a user (the e-Document holder) and verifying its authenticity.
Inspection System	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	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 that 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 a passport) [R22].
Issuing State	The Country issuing the e-Document [R22]
Logical Data Structure	The collection of groupings of DG's stored in the optional capacity expansion technology [R22]. The capacity expansion technology used is the e-Document's chip.

Logical e-Document	Data of the e-Document holder stored according to the LDS [R22] as specified by ICAO on the IC. It presents machine 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 and v. the other data according to LDS (EF.DG5 to EF.DG16).
Machine Readable Electronic document	Official document issued by a State or Organization which is used by the holder (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read [R22].
Machine Readable Zone	Fixed dimensional area located on the front of the e-Document Data Page or, in the case of the TD1, the back of the e-Document, containing mandatory and optional data for machine reading using OCR methods [R22].
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.
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 finger print and not to use iris images as optional biometric reference data.
Passive Authentication	Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by: i. the verification of the digital signature of the SO_D and ii. comparing the hash values of the read LDS data fields with the hash values contained in the SO_D.
Personalization	The process by which the portrait, signature and biographical data are applied to the document [R22].

Personalization Agent	The agent delegated by the Issuing State or Organization to personalize the e-Document for the holder by i. establishing the identity 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.
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 MRZ, iii. photographic image and iv. other data.
Pre-personalization Agent	The agent who performs pre-personalization by writing Pre-personalizatino Data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the Pre-personalization Agent (Phase 2) for traceability of non-personalized e-Document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization key pair.
Pre-personalized e-Document's chip	e-Document's chip equipped with a unique identifier, the Personalization keys, and a unique asymmetric Active Authentication Key Pair of the chip.
Presenter	A person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.
Primary Inspection System	An inspection system that contains a terminal for the contact or contactless communication with the e-Document's chip and does not implement the terminals part of the Basic Access Control Mechanism.
Receiving State or Organization	The Country or the Organization to which the e-Document holder is applying for entry or control [R22].
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R26].
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 [R16].
Unpersonalized e-Document	e-Document material prepared to produce an personalized e-Document containing an initialized and pre-personalized e-Document's chip.
User data	Data created by and for the user, that does not affect the operation of the TSF [R16].
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template [R22].
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

8.3 Technical References

[R1] **Arjo Systems**: *Security Target SOMA-c007 Machine Readable Electronic Document, EAC-PACE-AA, ref. TCAE160002*

[R2] **Arjo Systems**: *Security Target SOMA-c007 Machine Readable Electronic Document, Secure Signature Creation, ref. TCAE160003*

[R3] **Arjo Systems**: *Initialization Guidance for SOMA-c007 Machine Readable Electronic Document v2.1, ref. TCAE160012*

[R4] **Arjo Systems**: *Pre-personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160016*

[R5] **Arjo Systems**: *Personalization Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160017*

[R6] **Arjo Systems**: *User Guidance for SOMA-c007 Machine Readable Electronic Document ICAO Application v2.0, ref. TCAE160018*

[R7] **Arjo Systems**: *Secure Delivery Procedure, ref. TCAE110027*

[R8] **BSI**: *Certification report BSI-DSZ-CC-0891-V2-2016 for Infineon Security Controller M7892 design steps D11 and G12, with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from Infineon Technologies AG, 20 December 2016*

[R9] **BSI**: *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*

[R10] **BSI**: *Security IC Platform Protection Profile version 1.0 15 June, 2007; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035*

[R11] **BSI:** *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application ", Basic Access Control, Version 1.10, 25th March 2009, BSI-CC-PP-0055.*

[R12] **BSI**: *Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application ", Extended Access Control with PACE, Version 1.3.2, 5th December 2012, BSI-CC-PP-0056-V2-2012.*

[R13] **BSI**: *Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2nd November 2011, BSI-CC-PP-0068-V2-2011.*

[R14] **BSI**: *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, part 1 – eMRTDs with BAC/PACEv2 and EACv1, version 2.20, 26. February 2015*

[R15] **BSI**: *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, part 3 – Common Specifications, version 2.21, 21. December 2016*

[R16] **CCMB**: *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, version 3.1 rev.4, CCMB-2012-09-001*

[R17] **CCMB**: *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, September 2012, version 3.1 rev.4, CCMB-2012-09-002*

[R18] CCMB: *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, September 2012, version 3.1 rev 4, CCMB-2012-09-003*

[R19] EMV: *Card Personalization Specification – version 1.0, July 2003*

[R20] European Parliament: *Directive 1999/93/EC on a "Community framework for electronic signatures", December 1999*

[R21] EuroSmart: *Security IC Platform Protection Profile with Augmentation Packages version 1.0, ref. BSI-CC-PP-0084-2014, 13 01 2014*

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

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

[R24] IETF Network Working Group: *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.*

[R25] Infineon: *Public Security Target M7892 Design Steps D11 and G12, revision 1.7 as of 2016-11-16*

[R26] ISO/IEC: *International Standard 7816-4 2005 Information Technology – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange – January 15, 2005*

[R27] ISO/IEC: *International Standard 9797-1 1999 nformation Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*

[R28] ISO/IEC: *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics.*

[R29] ISO/IEC: *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface.*

[R30] ISO/IEC: *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.*

[R31] ISO/IEC: *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol.*

[R32] ISO/IEC: *International Standard 7816-2:2007 Identification cards - Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts*

[R33] ISO/IEC: *International Standard 10116:2006 – Information technology – Security techniques – Modes of operation for a n-bit block cipher, third edition 2006-02-01*

[R34] JIWG: *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.4, August 2015*

[R35] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology*

[R36] NIST: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 180-2, SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology – 2002 August 1*

[R37] NIST: *Federal Information Processing Standards Publication FIPS PUB 197, Specification fot the Advanced Encryption Standard (AES), 2001*

[R38] RSA Laboratories: *PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.*

[R39] RSA Laboratories: *PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.*

[R40] RSA Laboratories: *PKCS #15 v1.1: Cryptographic Token Information Syntax Standard*

[R41] ICAO: *Doc 9303, Machine Readable Travel Documents, Part 12: Public Key Infrastructure for MRTDs, Seventh Edition, 2015*

[R42] ISO/IEC: *International Standard 11770-2, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

[R43] NIST: FIPS PUB 180-4, Federal Information Processing Standards Publication, Secure Hash Standard (SHS), March 2012

Appendix A Platform identification

The IC on which the TOE is based, constituting the platform for its composite evaluation (cf. [R34]), consists of the secure microcontroller M7892 G12 with RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01, and Toolbox v2.03.008 libraries, developed and manufactured by Infineon. This IC has obtained a Common Criteria certification at Evaluation Assurance Level EAL6 augmented with ALC_FLR.1.

The current certification report of chip M7892 G12 is identified in the bibliography (cf. [R8]), and is associated with the following reference code:

BSI-DSZ-CC-0891-V2-2016

The current version of the public security target of the chip is identified in the bibliography, too (cf. [R25]).

END OF DOCUMENT