



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
EAC-PACE-AA

Public Version

Common Criteria version 3.1 revision 4
Assurance Level EAL5+

Version 1.0
Date 2017-09-21
Reference TCAE160020
Classification PUBLIC

Table of Contents

Abbreviations and Notations	8
1. Introduction	10
1.1 ST overview.....	10
1.2 ST reference.....	11
1.3 TOE reference.....	11
1.4 TOE overview.....	12
1.4.1 TOE definition	12
1.4.2 TOE usage and security features for operational use	13
1.4.3 Non-TOE hardware/software/firmware required by the TOE.....	16
1.5 TOE life cycle	17
1.5.1 Phase 1: Development.....	21
1.5.2 Phase 2: Manufacturing.....	22
1.5.3 Phase 3: Personalization.....	23
1.5.4 Phase 4: Operational use	24
1.6 TOE Description	25
1.6.1 Physical scope of the TOE.....	25
1.6.2 Other non-TOE physical components.....	25
1.6.3 Logical scope of the TOE	26
2. Conformance claims	32
2.1 Common Criteria Conformance Claim.....	32
2.2 Protection Profile Conformance Claim	32
2.3 Package Conformance Claim	32
2.4 Conformance Claim Rationale.....	32

3.	Security Problem Definition	40
3.1	Introduction	40
3.1.1	Assets	40
3.1.2	Subjects	43
3.2	Assumptions	48
3.3	Threats	50
3.4	Organizational Security Policies	55
4.	Security Objectives	59
4.1	Security Objectives for the TOE	59
4.2	Security Objectives for the Operational Environment	63
4.3	Security Objective Rationale	68
5.	Extended Components Definition	74
5.1	Definition of the family FAU_SAS	74
5.2	Definition of the family FCS_RND	74
5.3	Definition of the family FIA_API	75
5.4	Definition of the family FMT_LIM	76
5.5	Definition of the family FPT_EMS	78
6.	Security Requirements	80
6.1	Security Functional Requirements for the TOE	84
6.1.1	Class FAU Security Audit	85
6.1.2	Class FCS Cryptographic Support	85
6.1.3	Class FIA Identification and Authentication	96
6.1.4	Class FDP User Data Protection	108
6.1.5	Class FTP Trusted Path/Channels	114
6.1.6	Class FMT Security Management	115

6.1.7	Class FPT Protection of the Security Functions	125
6.2	Security Assurance Requirements for the TOE	129
6.3	Security Requirements Rationale.....	130
6.3.1	Security functional requirements rationale	130
6.3.2	Dependency Rationale.....	137
6.3.3	Security Assurance Requirements Rationale.....	143
6.3.4	Security Requirements – Mutual Support and Internal Consistency .	143
7.	TOE Summary Specification	145
7.1	Coverage of SFRs.....	145
7.1.1	SS.AUTH_IDENT Identification & Authentication.....	145
7.1.2	SS.SEC_MSG Secure data exchange	148
7.1.3	SS.ACC_CNTRL Storage and Access Control of Data Objects	149
7.1.4	SS.LFC_MNG Life cycle management.....	150
7.1.5	SS.SW_INT_CHECK Software integrity check of TOE’s assets	150
7.1.6	SS.SF_HW Security features provided by the hardware	151
7.1.7	SS.SIG_VER Verification of digital signatures	151
7.2	Assurance Measures.....	153
8.	References	156
8.1	Acronyms	156
8.2	Glossary	157
8.3	Technical References.....	165
Appendix A	Platform identification.....	169

List of Tables

Table 1-1	ST reference.....	11
Table 1-2	TOE reference.....	11
Table 1-3	Legend for deliveries not occurring between consecutive actors.....	18
Table 1-4	Roles Identification	20
Table 1-5	Identification of recipient actors for the guidance documentation of the TOE	21
Table 2-1	Source of assumptions, threats and OSPs.....	34
Table 2-2	Source of security objectives.....	34
Table 2-3	Modified/Added components	35
Table 2-4	Source of Security Functional Requirements.....	37
Table 2-5	Additions, iterations and changes to SFRs	38
Table 3-1	Primary assets.....	40
Table 3-2	Secondary assets.....	42
Table 3-3	Subjects and external entities according to PACE PP.....	44
Table 4-1	Security Objective Rationale	69
Table 5-1	Family FAU_SAS	74
Table 5-2	Family FCS_RND	75
Table 5-3	Family FIA_API	76
Table 5-4	Family FMT_LIM	77
Table 5-5	Family FPT_EMS	79
Table 6-1	Definition of security attributes	80
Table 6-2	Keys and certificates	82

Table 6-3	RSA algorithms for signature verification in Terminal Authentication	
([R13][R14])	95
Table 6-4	ECDSA algorithms for signature verification in Terminal Authentication	
([R13][R14])	95
Table 6-5	Overview of authentication SFRs	96
Table 6-6	Assurance requirements at EAL5+	129
Table 6-7	Coverage of Security Objective for the TOE by SFR	130
Table 6-8	Dependencies between the SFR for the TOE	138
Table 7-1	Summary of authentication mechanisms	146
Table 7-2	Coverage of SFRs by security services	152
Table 7-3	Assurance Requirements documentation	155

List of Figures

Figure 1-1 TOE life cycle	19
Figure 1-2 Smart card physical components	26
Figure 1-3 TOE architectural overview.....	27
Figure 3-1 Advanced Inspection Procedure	48

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.

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 [R27].

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 <i>not modified in the current stage</i>		Dedicated File <i>created in the current stage</i>
	System Object <i>not modified in the current stage</i>		Elementary File <i>not modified in the current stage</i>
	System Object <i>modified in the current stage</i>		Elementary File <i>modified in the current stage</i>
	System Object <i>optionally/conditionally modified in the current stage</i>		Elementary File <i>optionally/conditionally modified in the current stage</i>
	System Object <i>created in the current stage and left empty</i>		Elementary File <i>created in the current stage and left empty</i>
	System Object <i>created in the current stage and left empty</i>		Elementary File <i>created in the current stage and left empty</i>
	System Object <i>no longer available</i>		Elementary File <i>no longer available</i>
	System Object <i>optional/conditional</i>		Elementary File <i>optional/conditional</i>

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 7th ed. 2015 [R22][R23][R24], 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 [R45].

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

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

- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 7th ed. 2015 Part 11 [R23], and Terminal Authentication according to BSI TR-03110 [R13][R14],
- Password Authenticated Connection Establishment (PACE), according to ICAO Doc 9303 7th ed. 2015 Part 11 [R23],
- Active Authentication according to ICAO Doc 9303 7th ed. 2015 Part 11 [R23].

The TOE also supports:

- the Basic Access Control (BAC) as per ICAO Doc 9303-11 [R23], which is addressed by another ST [R1], and
- Secure Signature Creation (SSC), which is 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 - EAC-PACE-AA - Public Version
Version	1.0
Authors	Marco EVANGELISTA, Pasquale NOCE
Reference	TCAE160020

1.3 TOE reference

Table 1-2 TOE reference

TOE name	SOMA-c007 Machine Readable Electronic Document EAC-PACE-AA
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

This ST defines the security objectives and requirements for the contact based / contactless smart card of a machine readable electronic document based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment (PACE), Extended Access Control (EAC), Active Authentication (AA) and Chip Authentication (CA).

1.4.1 TOE definition

The TOE is an electronic document representing a contactless/contact smart card programmed according to the “Password Authenticated Connection Establishment” mechanism described in the ICAO Doc 9303 7th edition 2015 Part 11 [R23], which means amongst others according to the Logical Data Structure (LDS) defined in [R22], and additionally providing the Extended Access Control according to the ICAO Doc 9303-11 [R23] and BSI TR-03110 [R13][R14]. The communication between terminal and chip shall be protected by PACE using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [R12].

The TOE is composed of:

- the circuitry of the dual interface e-Document’s chip M7892 G12 (see Appendix A),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- 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 Profiles [R10][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.

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

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

For the ICAO application, the document holder can control access to his user data by consciously presenting his document to organizations deputed to perform inspection¹.

In the case of a secret PACE password, the document holder can exert further control over access to his data as in addition to his document, he must separately reveal the password in order to authorize inspection.

The document's chip is integrated into a physical (plastic or paper) substrate. The substrate is not part of the TOE. The tying-up of the document's chip to the plastic/paper document is achieved in accordance with physical and organizational security measures being within the scope of the current security target.

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

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

Additionally, the **e-Document** may bear:

- ii. visual (eye readable) biographical data and portrait of the holder,
- iii. a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ).

The authentication of the **presenter**² is based on:

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

¹ user authentication with PACE password, such as CAN or MRZ or shared secret, see [R23]

² The person presenting the **e-Document** to the Inspection System.

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

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

- the **physical part of the electronic document** in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the **e-Document** holder:
 - i. the biographical data on the biographical data page of the data surface,
 - ii. the printed data in the Machine-Readable Zone (MRZ),
 - iii. the printed portrait
- the **logical e-Document** as data of the document holder stored according to the Logical Data Structure as defined in [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 both³,
 - iv. the other data according to LDS (EF.DG5 to EF.DG16),
 - v. the Document security object (SO_D) and
 - vi. security data objects required for product management.

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

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

The logical **e-Documents** 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.

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

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

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

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

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

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

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

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

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

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

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

- i. The **e-Document**'s chip encrypts a nonce with the shared password, derived from the PACE password (MRZ, CAN or secret password) and transmits the encrypted nonce together with the domain parameters to the terminal;
- ii. The terminal recovers the nonce using the shared password. If this password is derived from MRZ or CAN, MRZ data or CAN data are physically read;
- iii. The **e-Document**'s chip and terminal computer perform a Diffie-Hellman key agreement together with the ephemeral domain parameters to create a shared

- secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.
- iv. Each party generates an authentication token, sends it to the other party and verifies the received token.

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

- v. the e-Document computes Chip Authentication Data, encrypts them, and sends them to the terminal;
- vi. the terminal recovers Chip Authentication Data and verifies the authenticity of the chip.

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

This security target requires the TOE to implement the Extended Access Control as defined in [R22][R13][R14] and additionally the Active Authentication as defined in [R23].

The Extended Access Control consists of two parts (i) the Chip Authentication and (ii) the Terminal Authentication Protocol Version 1 (v.1).

The Chip Authentication may be performed as part of the PACE protocol (see steps v. and vi. above), or as a distinct protocol (Chip Authentication protocol version 1). Both modes are detailed in section 4.4 of Doc 9303-11 [R23].

The Chip Authentication (i) authenticates the e-Document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore, Terminal Authentication v.1 can only be performed if either PACE-CAM or Chip Authentication Protocol v.1 have been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

The Active Authentication authenticates the e-Document to the inspection system.

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

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

1.5 TOE life cycle

The TOE life cycle is 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 1 *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.*

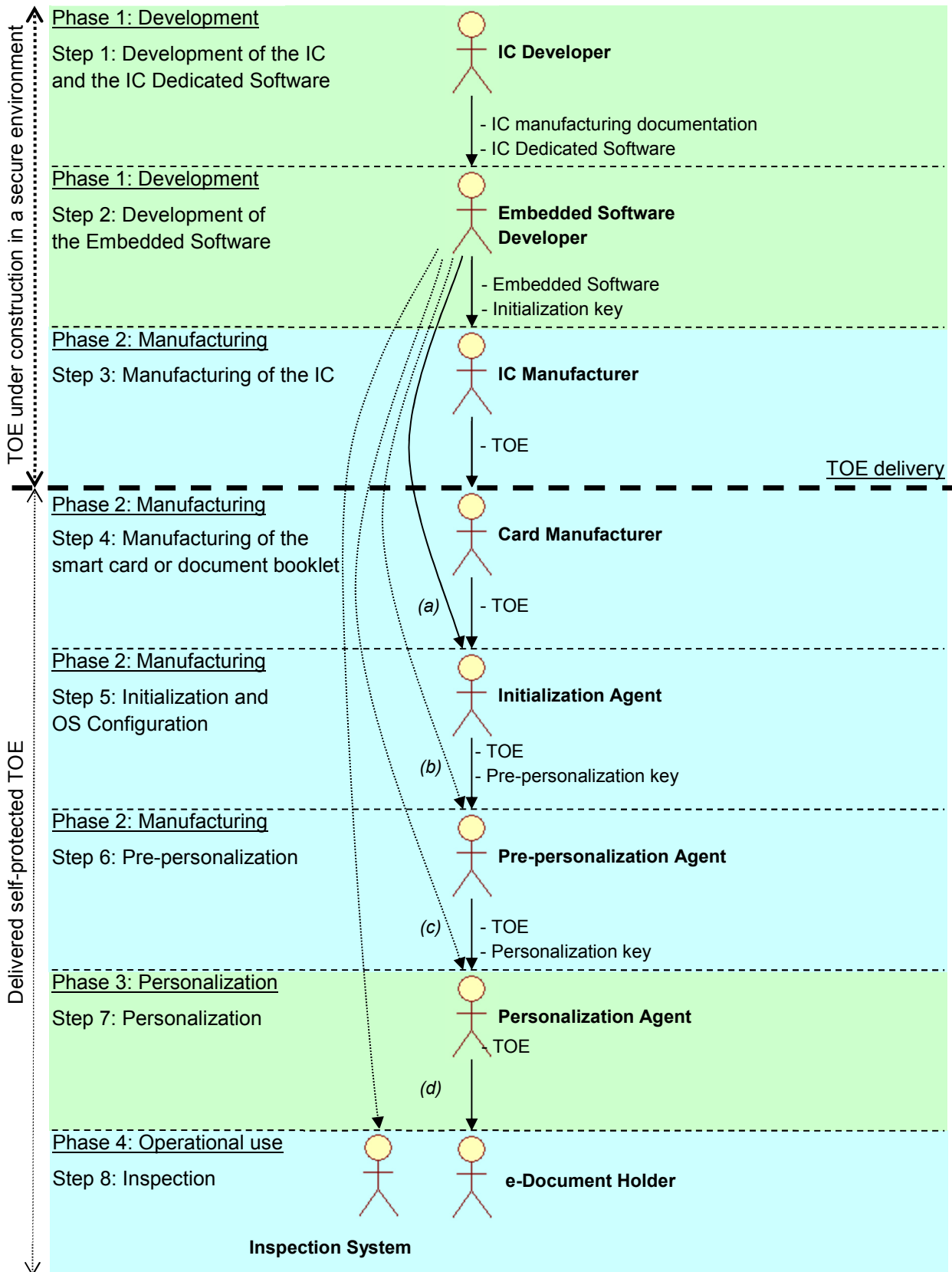
Figure 1-1 shows life cycle phases and steps. The picture also identifies the actors involved in each life cycle step. Direct deliveries of items between actors are represented with continuous lines, while deliveries in which intermediate actors may be in charge of receiving the exchanged items and forwarding 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)	<ul style="list-style-type: none"> • Initialization cryptograms • Initialization guidance
(b)	<ul style="list-style-type: none"> • Pre-personalization key • Pre-personalization guidance
(c)	<ul style="list-style-type: none"> • Personalization guidance
(d)	<ul style="list-style-type: none"> • 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 2 *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 3 *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 4 *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 [R24] finalizes the personalization of the genuine [e-Document](#) for the document holder.

Application Note 5 *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 6 *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 Personalization key(s) and the Chip Authentication Private Key (see [R23]).*

Application Note 7 *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 8 *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.

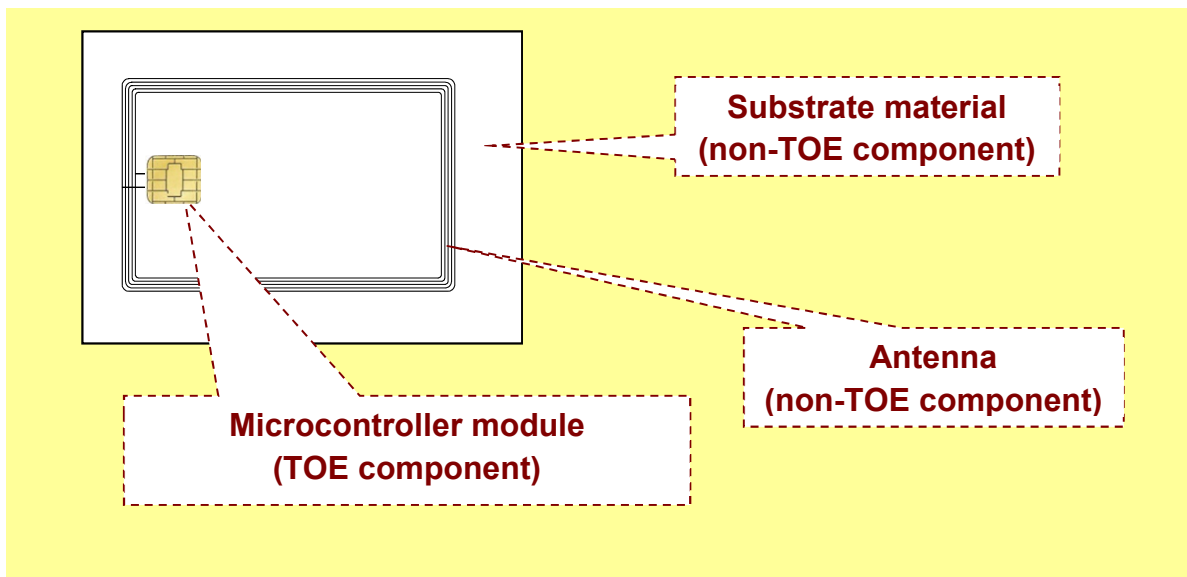
The TOE will be distributed according to the Secure Delivery Procedure [R46].

1.6.2 Other non-TOE physical components

The substrate and the antenna are not part of the TOE.

Figure 1-2 shows the physical components, distinguishing between TOE components and non-TOE components.

Figure 1-2 Smart card physical components



1.6.3 Logical scope of the TOE

The SOMA-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:

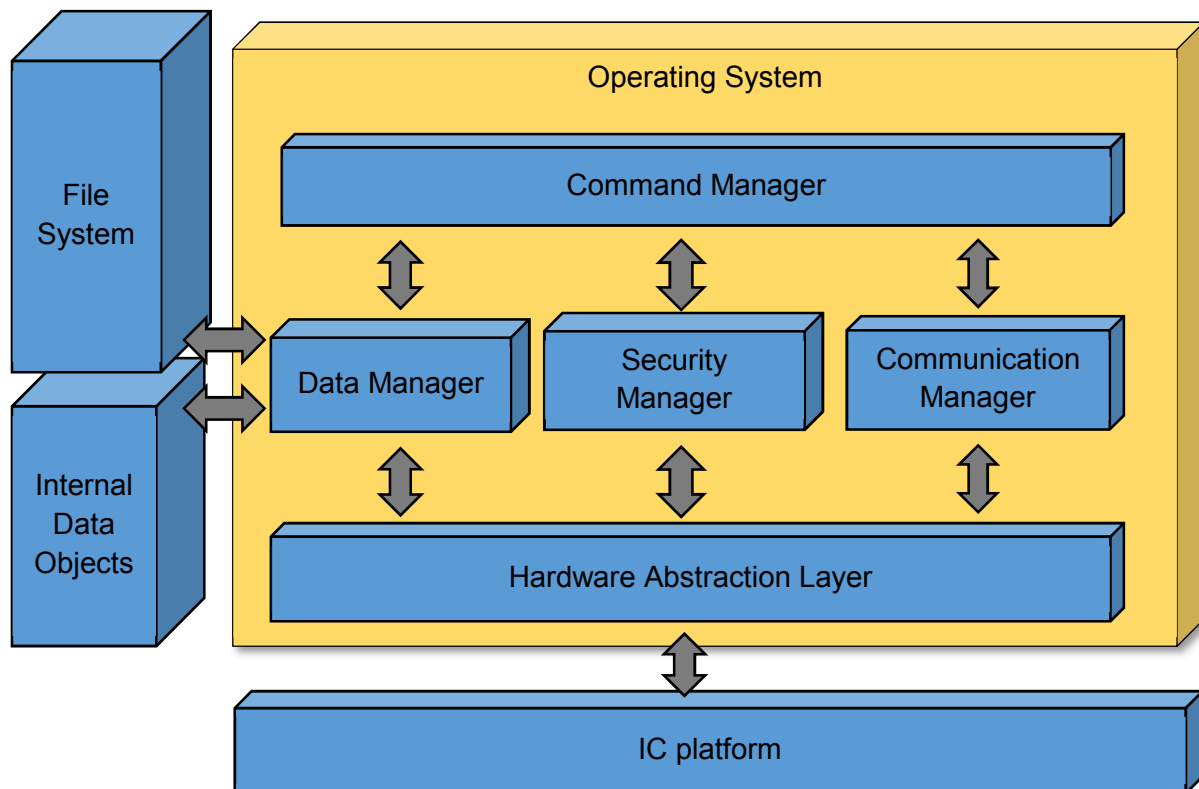
- Communication between internal objects
- Communication with external devices
- Data storage in the file system
- Execution of commands
- Cryptographic operations
- Management of the security policies

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 PACE mechanism

compliant to ICAO Doc 9303-11 [R23]. Access to sensitive data, i.e. DG3 and DG4 is allowed after the genuinity of the IC has been proven by means of the Chip Authentication mechanism defined in [R23] and after the user has proven his/her entitlement by means of the Terminal Authentication mechanism as defined in [R13][R14].

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 [R28].

The integrity of data stored under the LDS is checked by means of the Passive Authentication mechanism defined in [R23]. The Active Authentication mechanism defined in [R23] may be used as an alternative technique to prove the genuinity of the chip. However, access to less sensitive data requires the Chip Authentication mechanism. The Passive Authentication, PACE, EAC and Active 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 [R24].
3. The inspection system uses the verified Document Signer Public Key (K_{P_UDS}) to verify the signature of the Document Security Object (SO_D).
4. The inspection system reads relevant data groups from the IC.
5. The inspection system ensures that the contents of the data groups are authentic and unchanged by hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SO_D).

1.6.3.2 Password Authenticated Connection Establishment (PACE)

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

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

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

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

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

All the algorithm combinations (i.e. key agreement algorithms, mapping algorithms, block ciphers) and the standardized domain parameters specified in ICAO Doc 9303-11 [R23] are supported for PACE authentication.

1.6.3.3 Active Authentication

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

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

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

In accordance with ICAO Doc 9303 [R23], the ICAO application supports signature creation compliant with [R29], Digital Signature Scheme 1 for Active Authentication, with hash algorithm SHA-256 compliant with FIPS PUB 180-4 [R47] and keys of 2048 or 3072 bits.

1.6.3.4 Chip Authentication

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

The main differences with respect to Active Authentication are:

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

Details on Challenge Semantics are described in [R23].

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

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

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

In accordance with ICAO Doc 9303 [R23], the ICAO application supports Diffie-Hellman key agreement for Chip Authentication either on integer multiplicative groups (DH algorithm, cf. [R44]), with keys of 2048 bits, or on elliptic curve groups over prime fields (ECDH algorithm, cf. [R15]), with keys of 224, 256, 320, 384, 512, 521 bits.

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

1.6.3.5 Extended Access Control

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

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

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

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

Following BSI TR-03110 [R13][R14], the ICAO application supports Terminal Authentication with signature verification algorithm RSASSA-PSS (cf. [R43]), and ECDSA (cf. [R15]). Hash algorithm SHA-256 (cf. [R47]) and keys of 2048 or 3072 bits are supported in the RSA case, while hash algorithm SHA-256 (cf. [R47]) and keys of 224 or 256 bits are supported in the ECC case.

2. Conformance claims

2.1 Common Criteria Conformance Claim

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 (see Appendix A). This integrated circuit is certified against Common Criteria at the assurance level EAL6+ (cf. [R7]).

2.2 Protection Profile Conformance Claim

This ST claims strict conformance to:

- BSI-CC-PP-0056-V2-2012 Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), version 1.3.2 05th December 2012 [R11].
- BSI-CC-PP-0068-V2-2011-MA-01 Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.01, 22nd July 2014 [R12]

2.3 Package Conformance Claim

This Security Target claims conformance to:

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

2.4 Conformance Claim Rationale

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

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

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

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

With respect to the PPs, the role “MRTD Manufacturer” has been split into the roles “Card Manufacturer”, “Initialization Agent” and “Pre-personalization Agent”, acting in Phase 2 “Manufacturing”, respectively in Step 4 “Card Manufacturing”, Step 5 “Initialization” and Step 6 “Pre-personalization”. Note 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 4 of the EAC PP [R11]. At TOE delivery, there is no user data or machine readable data available. The EF.DG14 and EF.DG15 files, containing part of the user data, are written by the Pre-personalization Agent in Step 6 “Pre-Personalization” of Phase 2. The remaining user data as well as applicative files are written by the Personalization Agent, during Phase 3 “Personalization”.

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

The TOE provides a contact interface according to ISO/IEC 7816-2 [R36]; therefore, in addition to the contactless interface referred in the PPs, this ST makes also references to the contact interface.

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

The security problem definition includes the assets, the subjects, the assumptions, the threats and the organizational security policies of both PPs.

Table 2-1 specifies the source (PACE PP or EAC PP) of assumptions, threats and organizational security policies.

Table 2-1 Source of assumptions, threats and OSPs

	Source	
	PACE PP [R12]	EAC PP [R11]
Assumptions	<ul style="list-style-type: none"> • A.Passive_Auth 	<ul style="list-style-type: none"> • A.Insp_Sys • A.Auth_PKI
Threats	<ul style="list-style-type: none"> • T.Skimming • T.Eavesdropping • T.Tracing • T.Forgery • T.Abuse-Func • T.Information_Leakage • T.Phys-Tamper • T.Malfunction 	<ul style="list-style-type: none"> • T.Read_Sensitive_Data • T.Counterfeit
Organizational Security Policies	<ul style="list-style-type: none"> • P.Manufact • P.Pre-Operational • P.Card_PKI • P.Trustworthy_PKI • P.Terminal 	<ul style="list-style-type: none"> • P.Sensitive_Data • P.Personalization

The security objectives of both PPs are included in this ST.

Table 2-2 specifies the source (PACE PP or EAC PP) of security objectives for the TOE and of security objectives for the operational environment.

Table 2-2 Source of security objectives

	Source	
	PACE PP [R12]	EAC PP [R11]
Security Objectives for the TOE	<ul style="list-style-type: none"> • OT.Data_Integrity • OT.Data_Authenticity • OT.Data_Confidentiality • OT.Tracing • OT.Prot_Abuse-Func 	<ul style="list-style-type: none"> • OT.Sens_Data_Conf • OT.Chip_Aut_Proof

	<ul style="list-style-type: none"> • OT.Prot_Inf_Leak • OT.Prot_Phys-Tamper • OT.Prot_Malfunction • OT.Identification • OT.AC_Pers 	
Security Objectives for the operational environment	<ul style="list-style-type: none"> • OE.Personalization • OE-Passive_Auth_Sign • OE.Terminal • OE.e-Document_Holder • OE.Legislative_Compliance 	<ul style="list-style-type: none"> • OE.Chip_Auth_Key_e-Document • OE.Active_Auth_Key_e-Document • OE.Authoriz_Sens_Data • OE.Exam_e-Document • OE.Prot_Logical_e-Document • OE.Ext_Insp_Systems

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

Table 2-3 lists the assumptions, the security objectives and the policies that have been modified/added in this ST with respect to the PPs.

Table 2-3 Modified/Added components

Component	Definition	Operation
A.Insp_Sys	Inspection Systems for global interoperability	The definition has been extended to take into account the fact that if PACE-CAM is performed, there is no need to perform Chip Authentication v1.
OT.AC_Init	Access control for Initialization of e-Document	Added to take into account access control in Step 5 "Initialization".
OT.AC_Pre-pers	Access control for Pre-personalization of e-Document	Added to take into account access control in Step 6 "Pre-personalization".
OT.Active_Auth_Proof	Proof of e-Document's chip authenticity by Active Authentication	Added to cover the proof of IC authenticity for Basic Inspection Systems.
OE.Active_Auth_Key_e-Document	e-Document Active Authentication key	Added to cover the generation, signature and storage of the Active Authentication key pair, as well as the support to the Inspection System.

Component	Definition	Operation
OE.Exam_e-Document	Examination of the physical part of the e-Document	The definition from PP56 has been extended to take into account the fact that chip authenticity may also be proved by means of PACE-CAM.
OE.Initialization	Initialization of e-Document	Added to take into account responsibilities in Step 5.
OE.Pre-personalization	Pre-personalization of e-Document	Added to take into account responsibilities in Step 6.
OT.Tracing	Tracing e-Document	The definition from PP68 has been extended to take into account the presence of a contact interface.
OT.Identification	Identification of the TOE	Modified to specify that the Initialization Data are split into IC Initialization Data and TOE Initialization Data, that IC Initialization data include the Initialization key, and that TOE Initialization Data include the Pre-personalization keys.
OT.Chip_Auth_Proof	Proof of the e-Document's chip authenticity	The definition from PP56 has been extended to take into account the fact that chip authenticity may also be proved by means of PACE-CAM.
P.Manufact	Manufacturing of the e-Document's chip	Modified to specify the storage of e-Document's Manufacturer keys, DG14 and DG15.
P.Pre-operational	Pre-operational handling of the e-Document	The Initialization Agent and the Pre-personalization Agent have been added as subjects authorized by the e-Document Issuer.

The functional requirements described in section 6 of this ST include the SFRs of both the PACE PP [R12] and EAC PP [R11].

Table 2-4 specifies the source (PACE PP or EAC PP) of security functional requirements.

Table 2-4 Source of Security Functional Requirements

	Source	
	PACE PP [R12]	EAC PP [R11]
SFRs	<ul style="list-style-type: none"> • FCS_CKM.1/DH_PACE • FCS_CKM.4 • FCS_COP.1/PACE_ENC • FCS_COP.1/PACE_MAC • FCS_RND.1 • FIA_AFL.1/PACE • FIA_UID.1/PACE • FIA_UAU.1/PACE • FIA_UAU.4/PACE • FIA_UAU.5/PACE • FIA_UAU.6/PACE • FDP_ACC.1/TRM • FDP_ACF.1/TRM • FDP_RIP.1 • FDP_UCT.1/TRM • FDP_UIT.1/TRM • FTP_ITC.1/PACE • FAU_SAS.1 • FMT_SMF.1 • FMT_SMR.1/PACE • FMT_LIM.1 • FMT_LIM.2 • FMT_MTD.1/INI_ENA • FMT_MTD.1/INI_DIS • FMT_MTD.1/KEY_READ • FMT_MTD.1/PA • FPT_EMS.1 • FPT_FLS.1 • FPT_TST.1 • FPT_PHP.3 	<ul style="list-style-type: none"> • FCS_CKM.1/CA • FCS_COP.1/CA_ENC • FCS_COP.1/SIG_VER • FCS_COP.1/CA_MAC • FIA_UID.1/PACE • FIA_UAU.1/PACE • FIA_UAU.4/PACE • FIA_UAU.5/PACE • FIA_UAU.6/PACE • FIA_UAU.6/EAC • <u>FIA_API.1/CA</u> • FDP_ACC.1/TRM • FDP_ACF.1/TRM • FMT_SMR.1/PACE • FMT_LIM.1 • FMT_LIM.2 • FMT_MTD.1/CVCA_INI • FMT_MTD.1/CVCA_UPD • FMT_MTD.1/DATE • FMT_MTD.1/CAPK • FMT_MTD.1/KEY_READ • FMT_MTD.3 • FPT_EMS.1

In the above table, note the following points:

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

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

Table 2-5 Additions, iterations and changes to SFRs

Security Functional Requirement	Operation
FCS_CKM.1/CPS	<p>Iteration This iteration has been added to cover the generation of the session keys for the Pre-personalization Agent and for the Personalization Agent.</p>
FCS_CKM.1/GIM	<p>Iteration This iteration has been added to cover the generation of the Initialization Key.</p>
FIA_API.1/AA	<p>Iteration This iteration has been added to cover the proof of identity by means of Active Authentication.</p>
FIA_API.1/CAV1 FIA_API.1/CAM	<p>Iteration An iteration labelled “CAM” has been added to take into account PACE-CAM as an additional mechanism that the TOE must provide. The iteration label “CAV1” has replaced the iteration label “CA” in the original SFR from the PP to better distinguish it from the other iteration.</p>
FIA_AFL.1/Init FIA_AFL.1/Pre-pers FIA_AFL.1/Pers	<p>Iteration Iterations have been added to distinguish between authentication failure handling throughout pre-operational TOE life cycle.</p>
FCS_COP.1/AUTH	<p>Iteration This iteration has been added to cover the cryptographic mechanisms used in the authentication of the Initialization Agent, of the Pre-personalization Agent and of the Personalization Agent.</p>
FCS_COP.1/SIG_VER	<p>Addition of an Application Note An application note has been added concerning future-proof security.</p>

<p>FCS_COP.1/AA_SIGN</p>	<p>Iteration This iteration has been added to cover the signature of Active Authentication data.</p>
<p>FMT_MTD.1/AAPK</p>	<p>Iteration This iteration has been added to restrict the ability to cover the writing of the Active Authentication private key</p>
<p>FIA_UAU.4/PACE Single use authentication mechanisms – single use authentication of the Terminal by the TOE</p>	<p>Change of Application Note The application note now clarifies that this SFR also relates to the authentication of the Initialization Agent and of the Pre-personalization Agent (cf. Application Note 68).</p>
<p>FIA_UAU.5.2/PACE Multiple authentication mechanisms</p>	<p>Refinement The specification concerning Terminal Authentication takes into account the fact that session keys established during PACE-CAM may also be used. An alternative condition has been added for the TOE to accept authentication attempts by means of Terminal Authentication</p>
<p>FIA_UAU.6/EAC/CAV1 FIA_UAU.6/EAC/CAM</p>	<p>Iteration An iteration labelled “EAC/CAM” has been added to take into account PACE-CAM as an additional condition. The iteration label “CAV1” has been added to the original SFR from the PP, to distinguish it from the other iteration.</p>
<p>FPT_EMS.1.2 TOE Emanation</p>	<p>Refinement A refinement has been added to better specify access to data through contact interface.</p>
<p>FTP_ITC.1/CPS</p>	<p>Iteration This iteration has been added to require data to be exchanged through a secure channel in Pre-personalization and in Personalization.</p>

3. Security Problem Definition

Application Note 9 *With respect to the security problem definition defined in the protection profiles, this ST has some additions concerning the Active Authentication.*

3.1 Introduction

3.1.1 Assets

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

3.1.1.1 Assets to be protected according to PACE PP

The primary assets to be protected by the TOE as long as they are in scope of the TOE are listed in Table 3-1 (please refer to the glossary in chap. 7 for the term definitions).

Table 3-1 Primary assets

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

⁴ Though note ac data element stored on the TOE represents a secret, the specification [R23] anyway requires securing their confidentiality: only terminals authenticated according to [R23] can get access to the user data stored. They have to be operated according to P.Terminal.

2	User data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the ICAO application of the <i>electronic document</i> as defined in [R23] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [R23]). User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality ⁵ Integrity Authenticity
3	e-Document tracing data	Technical information about the current and previous locations of the e-Document gathered unnoticeable by the e-Document holder recognising the TOE not knowing any PACE password. TOE tracing data can be provided/gathered.	unavailability ⁶

Application Note 10 Please note that user data being referred to in the table above include, amongst other, individual-related (personal) data of the e-Document holder which also include his sensitive (i.e. biometric) data. Hence, the general security policy defined by the current PP also secures these specific e-Document holder’s data as stated in the table above.

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

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

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

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

Table 3-2 Secondary assets

Object No.	Asset	Definition	Property to be maintained by the current security policy
e-Document			
4	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way. This asset also covers “Authenticity of the MRTD’s chip” in [R10].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other on-secret material (Document Security Object SO _D containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	e-Document communication establishment authorisation data	Restricted-revealable ⁷ authorisation information for a humanuser being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be sent to it.	Confidentiality Integrity

Application Note 11 Since the **e-Document** does not support any secret document holder authentication data and the latter may reveal, if necessary, his or her verification values of the PACE password to an authorised person or device, a successful PACE

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

authentication of a terminal does not unambiguously mean that the *e-Document* holder is using TOE.

Application Note 12 *e-Document* communication establishment authorisation data are represented by two different entities: (i) reference information being persistently stored in the TOE and (ii) verification information being provided as input for the TOE by a human user as an authorisation attempt.

The TOE shall secure the reference information as well as – together with the terminal connected⁸ - the verification information in the “TOE ↔ terminal” channel, if it has to be transferred to the TOE. Please note that PACE passwords are not to be sent to the TOE.

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

3.1.1.2 Assets to be protected according to EAC PP

Logical *e-Document* sensitive User Data

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

Application Note 13 *Due to interoperability reasons the ICAO Doc 9303-11 [R23] requires that Basic Inspection Systems may have access to logical *e-Document* data DG1, DG2, DG5 to DG16. The TOE is not in certified mode according to this ST, if it is accessed using BAC [R23] (conformance to the BAC certification [R1] is kept, though). Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [R10]). If supported, it is therefore recommended to use PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform either PACE-CAM or Chip Authentication v.1 before getting access to data (except DG14), as these mechanisms are resistant to potential attacks.*

A sensitive asset is the following more general one.

Authenticity of the *e-Document*'s chip

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

3.1.2 Subjects

This security target considers the subjects defined in the PACE PP, and in the EAC PP.

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

The subjects considered in accordance with the PACE PP are listed in Table 3-3.

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

External Entity No.	Subject No.	Role	Definition
1	1	e-Document holder	A person for whom the e-Document Issuer has personalised the e-Document ⁹ . This entity is commensurate with e-Document Holder in [R10]. Please note that an e-Document holder can also be an attacker (see below external entity No.9).
2	-	e-Document presenter	A person presenting the e-Document to a terminal ¹⁰ and claiming the identity of the e-Document holder. This external entity is commensurate with “Traveller” in [R10]. Please note that an e-Document presenter can also be an attacker (see below external entity No.9).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contact or contactless interfaces. The role “Terminal” is the default role for any terminal being recognised by the TOE as not being PACE authenticated (“Terminal” is used by the e-Document presenter). This entity is commensurate with “Terminal” in [R10].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspection authority ¹¹ and verifying the e-Document presenter as the e-Document holder (for e-Document: by comparing the real biometric data (face) of the e-Document presenter with the stored biometric data (DG2) of the e-Document holder). BIS-PACE implements the terminal’s part of the PACE protocol and authenticates itself to the e-Document using a shared password (PACE password) and supports Passive Authentication.

⁹ i.e. this person is uniquely associated with a concrete electronic Passport

¹⁰ In the sense of [R23]

¹¹ Concretely, by a control officer

5	-	Document Signer (DS)	<p>An organization enforcing the policy of the CSCA and signing the Document Security Object stored on the e-Document for passive authentication.</p> <p>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [R24].</p> <p>This role is usually delegated to a Personalization Agent.</p>
6	-	Country Signing Certification Authority (CSCA)	<p>An organization enforcing the policy of the e-Document Issuer with respect to confirming correctness of user and TSF data stored in the e-Document. The CSCA represents the country specific root of the PKI for the e-Document and creates the Document Signer Certificates within this PKI.</p> <p>The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see [R24].</p>
7	4	Personalization Agent	<p>An organization acting on behalf of the e-Document Issuer to personalise the e-Document for its holder by some or all of the following activities (i) establishing the identity of the e-Document holder, (ii) enrolling the biometric reference data of the e-Document holder, (iii) writing a subset of these data on the physical e-Document (optical personalization) and storing them in the e-Document (electronic personalization) for the e-Document holder as defined in [R23], (iv) writing the document details data, (v) writing the initial TSF data data, (vi) signing the Document Security Object defined in [R22] (in the role of DS).</p> <p>Please note that the role “Personalization Agent” may be distributed among several institutions according to the operational policy of the e-Document Issuer.</p> <p>This entity is commensurate with “Personalization Agent” in [R22].</p>
8	5	Manufacturer	<p>Generic term collectively identifying the IC Manufacturer, the Card Manufacturer, the Initialization Agent and the Pre-personalization Agent. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase.</p>

			This entity commensurate with “Manufacturer” in [R10].
9	-	Attacker	<p>A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential.</p> <p>Please note that the attacker might “capture” any subject role recognised by the TOE.</p> <p>This external entity is commensurate to “Attacker” in [R10].</p>

Application Note 14 *The subject “Basic Inspection System with BAC” (BIS-BAC) is described in an other ST [R1].*

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

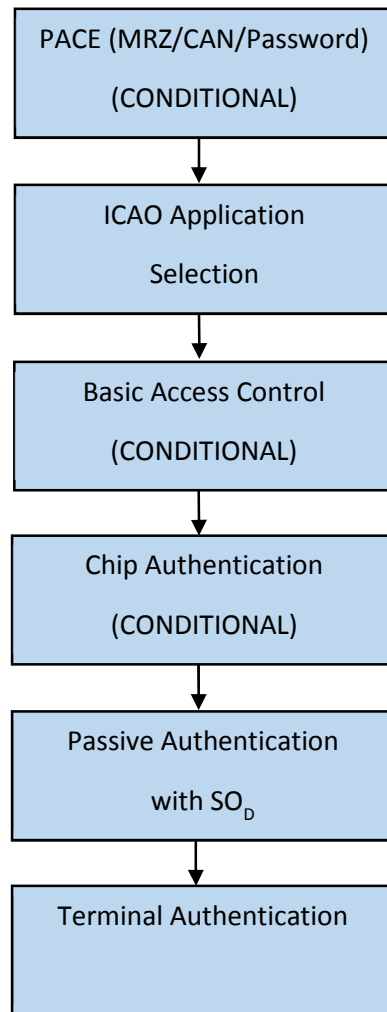
- Country Verifying Certification Authority:** The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the [e-Document](#). The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.
- Document Verifier:** The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the [e-Document](#) in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
- Terminal:** A terminal is any technical system communicating with the TOE through the contact or contactless interfaces.
- Inspection system (IS):** A technical system used by the border control officer of the receiving State (i) in examining an [e-Document](#) presented by the user and verifying its authenticity and (ii) verifying the [presenter](#) as [e-Document](#) holder.

The **Extended Inspection System (EIS)** performs the Advanced Inspection procedure (see Figure 3-1) and therefore (i) contains a terminal for the contact or contactless communication with the **e-Document**'s chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical **e-Document** either under PACE or BAC by optical reading the **e-Document** providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [R13][R14] and (v) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

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

Application Note 15 *An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged **e-Document**. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.*

Figure 3-1 Advanced Inspection Procedure



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

3.2 Assumptions

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

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

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical **e-Document**. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair.

The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer:

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

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

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

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [R23] and/or BAC [R10]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical [e-Document](#) under PACE or BAC and performs the Chip Authentication to verify the logical [e-Document](#) and establishes secure messaging. The Chip Authentication Protocol v.1 is skipped if PACE-CAM has previously been performed. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification: The assumption A.Insp_Sys does not confine the security objectives of the [R12] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE .

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

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

States or Organizations. The issuing States or Organizations distribute the public keys of their Country Verifying Certification Authority to their [e-Document](#)'s chip.

Justification: This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [R12] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

3.3 Threats

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

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

- **T.Skimming** **Skimming** **e-Document/Capturing** **Card-Terminal Communication**

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

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

Asset: confidentiality of logical [e-Document](#) data

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

Application Note 17 *The shared PACE password may be printed or displayed on the [e-Document](#). Please note that if this is the case, the password does not effectively represent a secret, but nevertheless it is restricted-revealable, cf. OE.[e-Document](#)_Holder.*

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

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

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

Asset: confidentiality of logical **e-Document** data

Application Note 18 *A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.*

- **T.Tracing** **Tracing e-Document**

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

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

Asset: privacy of the **e-Document** holder

Application Note 19 *This threat completely covers and extends “T.Chip-ID” from BAC PP [R10].*

Application Note 20 *A product using BAC (whatever the type of the inspection system is: BIS_BAC) cannot avert this threat in the context of the security policy defined in this ST.*

Application Note 21 *Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the **e-Document**'s chip (no Chip Authentication), a threat like T.Counterfeit (counterfeiting **e-Document**)¹² cannot be averted by the current TOE.*

¹² Such a threat might be formulated like: “An attacker produces an unauthorised copy or reproduction of a genuine **e-Document** to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine **e-Document** and copy them on another functionally appropriate chip to initiate this genuine **e-Document**. This violates the authenticity of the **e-Document** being used for authentication of a **e-Document** presenter as the **e-Document** holder.

- **T.Forgery** **Forgery of data**

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

Threat agent: having high attack potential

Asset: integrity of the [e-Document](#)

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 TOE operational phase in order (i) to manipulate or to disclose the *User Data stored in the TOE*, (ii) to manipulate or to disclose the *TSF-data stored in the TOE* or (iii) to manipulate (bypass, deactivate or modify) *soft-coded security functionality of the TOE*. This threat addresses the misuse of the functions for the initialisation and personalization in the operational phase after delivery to the [e-Document](#) holder.

Threat agent: having high attack potential, being in possession of one or more [e-Documents](#)

Asset: integrity and authenticity of the [e-Document](#), availability of the functionality of the [e-Document](#).

Application Note 22 *Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.*

- **T.Information_Leakage** **Information Leakage from [e-Document](#)**

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

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

Threat agent: having high attack potential

Asset: confidentiality User Data and TSF data of the [e-Document](#)

Application Note 23 *Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).*

- **T.Phys_Tamper Physical Tampering**

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

Threat agent: having high attack potential, being in possession of one or more legitimate [e-Documents](#)

Asset: integrity and authenticity of the [e-Document](#), availability of the functionality of the [e-Document](#), confidentiality of User Data and TSF-data of the [e-Document](#)

Application Note 24 *Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the [e-Document](#)) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the [e-Document](#)'s internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software*

design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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

Adverse action: An attacker may cause a malfunction the **e-Document**'s hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the **e-Document** outside the normal operating conditions, exploiting errors in the **e-Document**'s Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate **e-Documents**, having information about the functional operation

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

Application Note 25 *A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.*

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

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the **e-Document**'s chip. The attack T.Read_Sensitive_Data is similar to the threats T.Skimming (cf. [R1]) in respect of the attack path (communication interface) and the motivation (to get data stored on the **e-Document**'s chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the **e-Document**'s chip as private sensitive personal data

whereas the MRZ data and the portrait are visual readable on the physical **e-Document** as well.

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

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

- **T.Counterfeit Counterfeit of e-Document's chip**

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

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

Asset: authenticity of logical **e-Document** data

3.4 Organizational Security Policies

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

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

The IC Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the key for the authentication of the Initialization Agent.

The Initialization Agent configures the OS (TOE Initialization Data) and writes the key for the authentication of the Pre-personalization Agent.

The Pre-personalization Agent writes the Pre-Personalization Data which contains at least the Personalization key, the Chip Authentication public key (EF.DG14) and the Active Authentication public key (EF.DG.15).

The Initialization Agent and the Pre-personalization Agent are agents authorized by the Issuing State or Organization only.

- **P.Pre-Operational** **Pre-operational handling of the e-Document**

1. The e-Document Issuer issues the e-Document and approves it using the terminals complying with all applicable laws and regulations.
2. The e-Document Issuer guarantees correctness of the user data (amongst other of those, concerning the e-Document holder) and of the TSF-data permanently stored in the TOE.
3. The e-Document Issuer uses only such TOE's technical components (IC) which enable traceability of the e-Documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. section. 1.5 above.
4. If the e-Document Issuer authorises an Initialization Agent, a Pre-personalization Agent or a Personalization Agent to personalise the e-Document for e-Document holders, the e-Document Issuer has to ensure that the Initialization Agent, the Pre-personalization Agent and the Personalization Agent act in accordance with the e-Document Issuer's policy.

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

Application Note 26 *The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.*

1. The e-Document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the e-Document. For this aim, he runs a Country Signing Certification Authority (CSCA). The e-Document Issuer shall publish the CSCA Certificate (C_{CSCA}).
2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the e-Document Issuer by strictly secure means, see [R23]. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the e-Document Issuer, see [R24].
3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep

the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of [e-Documents](#).

- **P.Trustworthy_PKI** **Trustworthiness of PKI**

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

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

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

1. The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by [e-Document](#) holders as defined in [R23][R24].
2. They shall implement the terminal parts of the PACE protocol [R23], of the Passive Authentication [R23] and use them in this order¹³. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the [e-Document](#), [R22][R23]).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current PP.

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

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the [e-Document](#) holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the [e-Document](#) is presented to the inspection system (Extended

¹³ This order is commensurate with [R23]

Inspection Systems). The issuing State or Organization authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The **e-Document**'s chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

- **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.

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 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 pre-personalization 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.Data_Integrity Integrity of Data**

The TOE must ensure integrity of the User Data and the TSF-data¹⁴ stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

- **OT.Data_Authenticity Authenticity of Data**

¹⁴ Where appropriate, see Table 3-2 above

The TOE must ensure authenticity of the User Data and the TSF-data¹⁵ stored on it by enabling verification of their authenticity at the terminal-side¹⁶. The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)¹⁷

- **OT.Data_Confidentiality** **Confidentiality of Data**

The TOE must ensure confidentiality of the User Data and the TSF-data¹⁸ by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

- **OT.Tracing** **Tracing e-Document**

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

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

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

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

The TOE must provide protection against disclosure of confidential User Data and/or TSF-data stored and/or processed in the **e-Document**

¹⁵ Where appropriate, see Table 3-2 above

¹⁶ Verification of SO_D

¹⁷ Secure messaging after PACE authentication, see also [R23]

¹⁸ Where appropriate, see Table 3-2 above

- 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 27 *This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.*

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

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF-data, and the **e-Document**'s Embedded Software by means of

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

- **OT.Prot_Malfunction** **Protection against Malfunctions**

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

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

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

The TOE must provide means to store IC Initialization Data¹⁹, TOE Initialization Data and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide

¹⁹ Amongst other, IC identification data

a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the **e-Document**. The storage of the IC Initialisation 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).

- **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 [R22] and the TSF data can be written by an authorized Personalization Agent only. The logical **e-Document** data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalization of the document.

Application Note 28 *The OT.AC_Pers implies that the data of the LDS groups written during personalization for **e-Document** holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalization.*

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

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

- **OT.Chip_Auth_Proof** **Proof of **e-Document**'s chip authenticity**

The TOE must support the Inspection Systems to verify the identity and authenticity of the **e-Document**'s chip as issued by the identified issuing State or Organization by means of either the PACE-CAM as defined in [R23] or the Chip Authentication Version 1 as defined in [R13][R14]. The authenticity proof provided by **e-Document**'s chip shall be protected against attacks with high attack potential.

Application Note 29 *The OT.Chip_Auth_Proof implies the **e-Document**'s chip to have (i) a unique identity as given by the **e-Document**'s Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of **e-Document**'s chip i.e. a certificate for the Chip Authentication*

Public Key that matches the Chip Authentication Private Key of the *e-Document's* chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [R22] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

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

- **OT.Active_Auth_Proof Proof of *e-Document's* chip authenticity**

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

4.2 Security Objectives for the Operational Environment

e-Document Issuer as the general responsible

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

- **OE.Legislative_Compliance Issuing of the *e-Document***

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

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

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

- **OE.Passive_Auth_Sign Authentication of *e-Document* by Signature**

The *e-Document* Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the *e-Document* Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment,

and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained.

A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine **e-Documents** in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [R22]. The Personalization Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [R22]. The CSCA must issue its certificates exclusively to the rightful organizations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on **e-Document**.

- **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

- Create the OS configuration data and TSF data for the **e-Document**,
- initialize the **e-Document** together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

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

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

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

The **e-Document** Issuer must ensure that the Personalization Agent acting on his behalf (i) establish the correct identity of the **e-Document** holder and create the biographical data for the **e-Document**, (ii) enrol the biometric reference data of the **e-Document** holder, (iii) write a subset of these data on the physical Document (optical personalization) and store them in the **e-Document** (electronic personalization) for the **e-Document** holder as defined in [R22]²⁰,

²⁰ See also [R23].

(iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [R23] (in the role of a DS).

Terminal operator: Terminal's receiving branch

- **OE.Terminal Terminal operating**

The terminal operators must operate their terminals as follows:

1. The related terminals (basic inspection systems, cf. above) are used by terminal operators and by **e-Document** holders as defined in [R23].
2. The related terminals implement the terminal parts of the PACE protocol [R23], of the Passive Authentication [R23] (by verification of the signature of the Document Security Object) and use them in this order²¹. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the **e-Document** (determination of the authenticity of data groups stored in the **e-Document**, [R23]).
5. The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Application Note 30 *OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [R10].*

e-Document holder Obligations

- **OE.e-Document_Holder e-Document holder Obligations**

²¹ This order is commensurate with [R23]

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

Issuing State or Organization

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

- **OE.Chip_Auth_Key_e-Document** **e-Document Authentication Key**

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

Justification: This security objective for the operational environment is needed to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication which is one of the features of the TOE described only in this Security Target.

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

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

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

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

- **OE.Active_Auth_Key_e-Document** **e-Document Active Authentication key**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the **e-Document's** Active Authentication Key Pair, (ii) sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or Organizations to verify the authenticity of the **e-Document's** chip used for genuine **e-Document** by certification of the Active Authentication Public Key by means of the Document Security Object.

Receiving State or Organization

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

- **OE.Exam_e-Document** **Examination of the physical part of the e-Document**

The inspection system of the receiving State or Organization must examine the **e-Document** presented by the **user** to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the **e-Document**. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of PACE [4] and/or the Basic Access Control [6]. Extended Inspection Systems perform additionally to these points the Chip Authentication as either part of PACE-CAM or as Chip Authentication Protocol Version 1 to verify the Authenticity of the presented **e-Document's** chip.

Justification: This security objective for the operational environment is needed in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication as either part of PACE-CAM or as Chip Authentication protocol v.1. OE.Exam_e-Document also repeats partly the requirements from above OE.Terminal and therefore also counters T.Forgery and A.Passive_Auth. This is done because this ST introduces the Extended Inspection System, which is needed to handle the features of a **e-Document** with Extended Access Control.

- **OE.Prot_Logical_e-Document** **Protection of data from the logical e-Document**

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

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

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

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

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

4.3 Security Objective Rationale

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

Table 4-1 Security Objective Rationale

	OT.Sens_Data_Conf	OT.Chip_Aut_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.Chip_Auth_Key_e-Document	OE.Active_Auth_Key_e-Document	OE.Authoriz_Sens_Data	OE.Exam_e-Document	OE.Prot_Logical_e-Document	OE.Ext_Insp_Systems	OE.Initialization	OE.Pre-personalization	OE.Personalization	OE.Passive_Auth_Sign	OE.Terminal	OE.e-Document_Holder	OE.Legislative_Compliance
T.Read_Sensitive_Data	X																X			X								
T.Counterfeit		X	X													X	X		X									
T.Skimming							X	X	X																		X	
T.Eavesdropping								X																				
T.Tracing										X																X		
T.Abuse-Func											X																	
T.Information_Leakage												X																
T.Phys-Tamper														X														
T.Malfunction															X													
T.Forgery				X	X	X	X	X			X			X				X			X	X	X	X	X	X		
P.Sensitive_Data	X																X			X								
P.Personalization						X							X										X					
P.Manufact				X	X								X								X	X						
P.Pre-Operational				X	X	X							X								X	X	X					X
P.Terminal																			X							X		
P.Card_PKI																									X			
P.Trustworthy_PKI																									X			
A.Insp_Sys																			X	X								
A.Auth_PKI																		X			X							
A.Passive_Auth																			X						X			

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

The threat **T.Skimming** addresses accessing the User Data (stored on the TOE or transferred between the TOE and the terminal) using the TOE's contact or contactless interfaces. This threat is countered by the security objectives **OT.Data_Integrity**, **OT.Data_Authenticity**, and **OT.Data_Confidentiality** through the PACE authentication. The objective **OE.e-Document_Holder** ensures that a PACE session can only be

established either by the **e-Document** holder itself or by an authorised person or device, and, hence, cannot be captured by an attacker.

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

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

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

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

The threats **T.Information_Leakage**, **T.Phys-Tamper**, and **T.Malfunction** are typical for integrated circuits like smart cards under direct attack with high attack potential. The

protection of the TOE against these threats is obviously addressed by the directly related security objectives **OT.Prot_Inf_Leak**, **OT.Prot_Phys-Tamper**, and **OT.Prot_Malfunction**, respectively.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The assumption **A.Passive_Auth** “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** “Authentication of **e-Document** by Signature” from PACE PP [R12] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by **OE.Exam_e-Document** “Examination of the physical part of the **e-Document**”.

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

5. Extended Components Definition

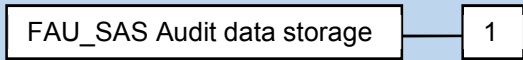
This ST uses components defined as extensions to CC part 2 [R17]. These components are drawn from PACE PP [R12] and from EAC PP [R11].

5.1 Definition of the family FAU_SAS

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

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

Table 5-1 Family FAU_SAS

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

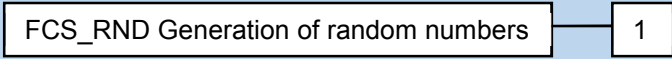
5.2 Definition of the family FCS_RND

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

component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

Table 5-2 Family FCS_RND


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

5.3 Definition of the family FIA_API

To describe the security requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [R11]. This family describes the functional requirements for the proof of a the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application Note 31 *The other families of the Class FIA describe only the authentication verification of users’ identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the CC part 2 (cf. [R18] “Explicitly stated IT security requirements (APE_SRE)” from a TOE point of view.*

Table 5-3 Family FIA_API

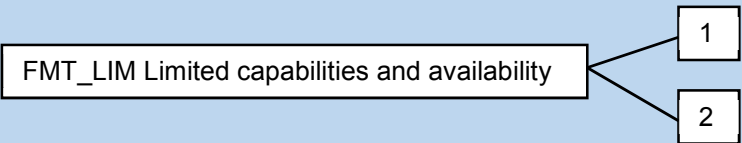
FIA_API Authentication Proof of Identity	
<i>Family behaviour:</i>	This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.
<i>Component leveling:</i>	
FIA_API.1	Authentication Proof of Identity.
<i>Management:</i>	The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
<i>Audit:</i>	There are no actions defined to be auditable.
FIA_API.1	Authentication Proof of Identity
<i>Hierarchical to:</i>	No other components
<i>Dependencies:</i>	No Dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: <i>authentication mechanism</i>] to prove the identity of the [assignment: <i>authorized user or rule</i>].

5.4 Definition of the family FMT_LIM

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

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

Table 5-4 Family FMT_LIM

FMT_LIM Limited capabilities and availability	
<i>Family behaviour:</i>	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.
<i>Component leveling:</i>	
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.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	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.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.
FMT_LIM.1	Limited capabilities
<i>Hierarchical to:</i>	No other components
<i>Dependencies:</i>	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: <i>Limited capability and availability policy</i>].
FMT_LIM.2	Limited availability
<i>Hierarchical to:</i>	No other components
<i>Dependencies:</i>	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: <i>Limited capability and availability policy</i>].

Application Note 32 *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*

- 1. the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced*

or conversely

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

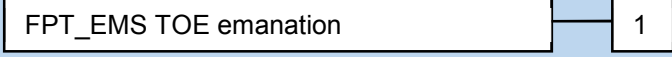
The combination of both requirements shall enforce the related policy.

5.5 Definition of the family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [R11].

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

Table 5-5 Family FPT_EMS

FPT_EMS TOE Emanation	
<i>Family behaviour:</i>	This family defines requirements to mitigate intelligible emanations.
<i>Component leveling:</i>	
FPT_EMS.1	TOE emanation has two constituents: <ul style="list-style-type: none"> • FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. • FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
<i>Management:</i>	There are no management activities foreseen.
<i>Audit:</i>	There are no actions defined to be auditable.
FPT_EMS.1	TOE Emanation
<i>Hierarchical to:</i>	No other components
<i>Dependencies:</i>	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: <i>types of emissions</i>] in excess of [assignment: <i>specified limits</i>] enabling access to [assignment: <i>list of types of TSF data</i>] and [assignment: <i>list of types of user data</i>].
FPT_EMS.1.2	The TSF shall ensure [assignment: <i>type of users</i>] are unable to use the following interface [assignment: <i>type of connection</i>] to gain access to [assignment: <i>list of types of TSF data</i>] and [assignment: <i>list of types of user data</i>].

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. Selections that have been made by the ST author are denoted as **bold underlined text** and the original text of the component is given by a footnote.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text. Assignments that have been made by the ST author are denoted as **bold underlined text** and the original text of the component is given by a footnote. In some cases, the assignment made by the PP authors defines a selection performed by the ST author. Thus this text is underlined and italicized like *this*.

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

The definition of the subjects “Manufacturer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section Application Note 9. 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 “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [R17]. The operation “load” is synonymous to “import” used in [R17].

Table 6-1 provides the definition of security attributes.

Table 6-1 Definition of security attributes

Security attribute	Values	Meaning
--------------------	--------	---------

Terminal authentication status	None (any Terminal)	Default role (i.e. without authorisation after start-up)
	CVCA	Roles defined in the certificate used for authentication (cf. [R13][R14]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	Roles defined in the certificate used for authentication (cf. [R13][R14]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	Roles defined in the certificate used for authentication (cf. [R13][R14]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 and TA v.1
	IS	Roles defined in the certificate used for authentication (cf. [R13][R14]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [R13][R14])
	DG3 (Fingerprint)	Read access to DG3: (cf. [R13][R14])
	DG3(Fingerprint)/DG4 (Iris)	Read access to DG3 and DG4: (cf. [R13][R14])

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

Table 6-2 Keys and certificates

Name	Data
Country Signing Certification Authority Key Pair and Certificate	Country Signing Certification Authority of the e-Document Issuer signs the Document Signer Public Key Certificate (C _{DS}) with the Country Signing Certification Authority Private Key (SK _{CSCA}) and the signature will be verified by receiving terminal with the Country Signing Certification Authority Public Key (PK _{CSCA}) The CSCA also issues the self-signed CSCA Certificate (C _{CSCA}) to be distributed by strictly secure diplomatic means, see. [R24].
Document Signer Key Pairs and Certificates	The Document Signer Certificate C _{DS} is issued by the Country Signing Certification Authority. It contains the Document Signer Public Key (PK _{DS}) as authentication reference data. The Document Signer acting under the policy of the CSCA signs the Document Security Object (SO _D) of the e-Document with the Document Signer Private Key (SK _{DS}) and the signature will be verified by a terminal as the Passive Authentication with the Document Signer Public Key (PK _{DS}).
PACE Session Keys (PACE-K _{MAC} , PACE-K _{ENC})	Secure messaging AES keys for message authentication (CMAC-mode) and for message encryption (CBC-mode) or Triple-DES ²² Keys for message authentication and message encryption (both CBC) agreed between the TOE and a terminal as result of the PACE Protocol, see [R23].
PACE authentication ephemeral key pair (ephem-SK _{PICC-PACE} , ephem-PK _{PICC-PACE})	The ephemeral PACE Authentication Key Pair (ephem-SK _{PICC-PACE} , ephem-PK _{PICC-PACE}) is used for Key Agreement Protocol: Diffie-Hellman (DH) according to PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03110 [R13][R14], cf [R23].
Ephem-PK _{PICC-PACE}	PKCS#3 or Elliptic Curve Diffie-Hellman (ECDH; ECKA key agreement algorithm) according to TR-03111 [R15], cf. [R23].
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

²² Usage of the algorithm Triple-DES is deprecated.

Country Verifying Certification Authority Private Key (SK _{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK _{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK _{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK _{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK _{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C _{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [R13][R14] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK _{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C _{DV})	The Document Verifier Certificate C _{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK _{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C _{IS})	The Inspection System Certificate (C _{IS}) issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK _{IS}) () the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK _{ICC} , PK _{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [11].
Chip Authentication Public Key (PK _{ICC})	The Chip Authentication Public Key (PK _{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical e-Document and used by the inspection system for Chip Authentication Version 1 of the e-Document's chip. It is part of the user data provided by the TOE for the IT environment.

Chip Authentication Private Key (SK _{ICC})	The Chip Authentication Private Key (SK _{ICC}) is used by the TOE to authenticate itself as authentic e-Document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical e-Document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key.
Chip Authentication Session Keys	Secure Messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
Active Authentication Key Pair	The Active Authentication Key Pair (SK _{AA} , PK _{AA}) is used for the Active Authentication mechanism in accordance with [R23].
Active Authentication Public Key (PK _{AA})	The Active Authentication Public Key (PK _{AA}) is stored in the EF.DG15. These keys are used by Inspection Systems to confirm the genuinity of the e-Document's chip.
Active Authentication Private Key (SK _{AA})	The Active Authentication Private Key (SK _{AA}) is used by the TOE to authenticate itself as genuine e-Document's chip.

Application Note 33 *The Country Verifying Certification Authority identifies a Document Verifier as “domestic” in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as “foreign” in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From e-Document's point of view the domestic Document Verifier belongs to the issuing State or Organization.*

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 <u>the Manufacturer</u> ²³ with the capability to store <u>the Initialization and Pre-personalization Data</u> ²⁴ in the audit records.
-------------	---

Application Note 34 *The Manufacturer role is the default user identity assumed by the TOE in the life cycle ‘manufacturing’. The IC manufacturer, the Initialization Agent and the Pre-personalization Agent in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF-Data into the TOE. The audit records are write-only-once data of the [e-Document](#) (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).*

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/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

²³ [assignment: *authorised user*]

²⁴ [assignment: *list of audit information*]

FCS_CKM.1.1/ GIM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>Initialization Key Generation Algorithm</u> ²⁵ and specified cryptographic key sizes <u>256 bit</u> ²⁶ that meet the following: <u>none</u> ²⁷
---------------------	---

Application Note 35 *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.*

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 <u>CPS Keys Generation Algorithm</u> ²⁸ and specified cryptographic key sizes <u>112 bit</u> ²⁹ that meet the following: <u>[R19], section 5.2</u> ³⁰
---------------------	---

Application Note 36 *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 keys in phase 2 and the Personalization keys in phase 3) and a sequence counter provided by the IC card to the pre-personalization terminal or to the personalization terminal in response to an INITIALIZE UPDATE command.*

²⁵ [assignment: cryptographic key generation algorithm]

²⁶ [assignment: cryptographic key sizes]

²⁷ [assignment: list of standards]

²⁸ [assignment: cryptographic key generation algorithm]

²⁹ [assignment: cryptographic key sizes]

³⁰ [assignment: list of standards]

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled but justified.
Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

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

<p>FCS_CKM.1.1/ DH_PACE</p>	<p>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:</p> <ol style="list-style-type: none"> 1. Diffie-Hellman Protocol compliant to PKCS#3 [R44]³¹ and specified cryptographic key sizes: 2048 bits³², and 2. ECDH compliant to [R15]³³ and specified cryptographic key sizes: 224, 256, 320, 384, 512, 521 bits³⁴, <p>that meet the following: [R23]³⁵.</p>
---------------------------------	--

Application Note 37 *The TOE generates a shared secret value K with the terminal during the PACE protocol, see [R23]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R44]) or on the ECDH compliant to TR-03111 [R15] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [R23] and [R15] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}) according to [R23] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.*

Application Note 38 *FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R23].*

³¹ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111]

³² [assignment: cryptographic key sizes]

³³ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111]

³⁴ [assignment: cryptographic key sizes]

³⁵ [assignment: list of standards]

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

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA	<p>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:</p> <ol style="list-style-type: none"> 1. Diffie-Hellman³⁶ and specified cryptographic key sizes: 2048 bits³⁷, that meet the following: <u>based on the Diffie-Hellman key derivation protocol compliant to [R44] and [R13][R14]</u>³⁸. or 2. ECDH³⁹ and specified cryptographic key sizes: 224, 256, 320, 384, 512, 521 bits⁴⁰, that meet the following: <u>based on an ECDH protocol compliant to [R15]</u>⁴¹.
----------------	---

Application Note 39 *FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [R13][R14].*

Application Note 40 *The TOE generates a shared secret value with the terminal during the Chip Authentication protocol Version 1, see [R13][R14]. This protocol may be based on the Diffie-Hellman-Protocol compliant to PKCS#3 (i.e. modulo arithmetic based cryptographic algorithm, cf. [R44]) or on the ECDH compliant to TR-03111 [R15] (i.e. the elliptic curve cryptographic algorithm - cf. [R15] for details). The shared secret value is used to derive the Chip Authentication session keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [R13][R14]).*

³⁶ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111]

³⁷ [assignment: cryptographic key sizes]

³⁸ [assignment: list of standards]

³⁹ [selection: based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to BSI TR-03111]

⁴⁰ [assignment: cryptographic key sizes]

⁴¹ [assignment: list of standards]

Application Note 41 *The TOE implements the hash functions SHA-1 and SHA-256 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. However, usage of the hash function SHA-1 is deprecated. The TOE implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (cf. [R13][R14] for details).*

Application Note 42 *Chip Authentication session keys are not generated if PACE-CAM has been performed, as in this case Chip Authentication protocol version 1 is skipped.*

6.1.2.2 FCS_CKM.4 Cryptographic key destruction – Session keys

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

FCS_CKM.4 Cryptographic key destruction – Session keys

Hierarchical to: No other components.

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

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: <u>physical deletion by overwriting the memory data with zeros</u> ⁴² that meets the following: <u>none</u> ⁴³ .
-------------	--

Application Note 43 *The TOE shall destroy any session keys in accordance with FCS_CKM.4 after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA. The TOE shall also destroy the Initialization Key.*

⁴² [assignment: cryptographic key destruction method]

⁴³ [assignment: list of standards]

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/AUTH Cryptographic operation – Authentication

Hierarchical to: No other components.

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

FCS_COP.1.1/AUTH	The TSF shall perform <u>symmetric authentication – encryption and decryption</u> ⁴⁴ in accordance with a specified cryptographic algorithm <u>Triple-DES and AES</u> ⁴⁵ and cryptographic key sizes: <u>112 bit for Triple-DES and 256 bit for AES</u> ⁴⁶ that meet the following: <u>FIPS 46-3 and FIPS 197</u> ⁴⁷
------------------	--

Application Note 44 *This SFR requires the TOE to implement the cryptographic primitive AES in CBC mode for authentication attempt of a terminal as Initialization Agent in Step 5: Initialization of Phase 2: Manufacturing, according to the mechanism described in the Initialization Guidance [R3].*

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

FCS_COP.1/AA_SIGN Cryptographic operation – Signature for Active Authentication

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

⁴⁴ [assignment: list of cryptographic operations]

⁴⁵ [selection: Triple-DES, AES]

⁴⁶ [selection: 112, 128, 168, 19, 256]

⁴⁷ [selection: FIPS 46-3, FIPS 197]

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ AA_SIGN	The TSF shall perform <u>digital signature for Active Authentication data</u> ⁴⁸ in accordance with a specific cryptographic algorithm <u>RSA with SHA-256</u> ⁴⁹ and cryptographic key sizes <u>2048 and 3072 bits</u> ⁵⁰ that meet the following: <u>the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital Signature scheme 1 [R29]) used for Active Authentication defined by ICAO Doc 9303-11 [R23]</u> ⁵¹ .
-------------------------	--

Application Note 46 *This SFR has been added by the ST author to specify the cryptographic algorithm and key sizes used by the TOE to perform an Active Authentication in accordance with ICAO Doc 9303-11 [R23].*

Application Note 47 *For RSA cryptography the TOE makes use of the cryptographic library embedded in the chip M7892.*

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption/Decryption AES/Triple-DES for PACE protocol

Hierarchical to: No other components.

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

FCS_COP.1.1/ PACE_ENC	The TSF shall perform <u>secure messaging – encryption and decryption</u> ⁵² in accordance with a specified cryptographic algorithm <u>AES and Triple-DES</u> in CBC mode ⁵³ and cryptographic
--------------------------	--

⁴⁸ [assignment: *list of cryptographic operations*]

⁴⁹ [assignment: *cryptographic algorithm*]

⁵⁰ [assignment: *cryptographic key sizes*]

⁵¹ [assignment: *list of standards*]

⁵² [assignment: *list of cryptographic operations*]

⁵³ [selection: *AES, Triple-DES*]

	key sizes 112 (for Triple-DES) , and 128, 192 and 256 bit (for AES) ⁵⁴ that meet the following: <u>compliant to [R23]⁵⁵</u> .
--	---

Application Note 48 *This SFR requires the TOE to implement the cryptographic primitive AES and Triple-DES for secure messaging with encryption of the transmitted data and encryption of the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to FCS_CKM.1/DH_PACE (PACE-K_{ENC}).*

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

FCS_COP.1/PACE_MAC Cryptographic operation – MAC for PACE protocol

Hierarchical to: No other components.

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

FCS_COP.1.1/ PACE_MAC	The TSF shall perform <u>secure messaging – message authentication code</u> ⁵⁶ in accordance with a specified cryptographic algorithm CMAC and Retail MAC ⁵⁷ and cryptographic key sizes 112, 128, 192 and 256 bit ⁵⁸ that meet the following: <u>compliant to [R23]⁵⁹</u> .
--------------------------	--

Application Note 50 *This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with [4] the (two-key) Triple-DES could be used in Retail mode for secure messaging. However, note that usage of Triple-DES is deprecated.*

⁵⁴ [assignment: cryptographic key sizes]

⁵⁵ [assignment: list of standards]

⁵⁶ [assignment: list of cryptographic operations]

⁵⁷ [selection: CMAC, Retail-MAC]

⁵⁸ [selection: 112, 128, 192, 256]

⁵⁹ [assignment: list of standards]

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption/Decryption for CA protocol

Hierarchical to: No other components.

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

FCS_COP.1.1/ CA_ENC	The TSF shall <u>perform secure messaging – encryption and decryption</u> ⁶⁰ in accordance with a specified cryptographic algorithm <u>AES and Triple-DES</u> ⁶¹ and cryptographic key sizes <u>112 (for Triple-DES) and 128, 192 and 256 bit (for AES)</u> ⁶² that meet the following: <u>ICAO Doc 9303-11 [R23]</u> ⁶³ .
------------------------	--

Application Note 51 *This SFR requires the TOE to implement the cryptographic primitives (i.e. Triple-DES and AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication according to the FCS_CKM.1/CA.*

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

FCS_COP.1/CA_MAC Cryptographic operation – MAC for CA protocol

Hierarchical to: No other components.

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

⁶⁰ [assignment: *list of cryptographic operations*]

⁶¹ [assignment: *cryptographic algorithm*]

⁶² [assignment: *cryptographic key sizes*]

⁶³ [assignment: *list of standards*]

FCS_COP.1.1/ CA_MAC	The TSF shall perform <u>secure messaging – message authentication code</u> ⁶⁴ in accordance with a specified cryptographic algorithm CMAC and Retail MAC ⁶⁵ and cryptographic key sizes 112, 128, 192 and 256 bit ⁶⁶ that meet the following: ICAO Doc 9303-11 [R23] ⁶⁷ .
------------------------	---

Application Note 53 This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication performed either part of PACE-CAM or Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Initialization Agent, or Personalization Agent by means of the authentication mechanism.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by e-Document

Hierarchical to: No other components.

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

FCS_COP.1.1/SIG_VER	The TSF shall perform <u>digital signature verification</u> ⁶⁸ in accordance with a specified cryptographic algorithm 1. RSA as specified in Table 6-3 ⁶⁹ and cryptographic key sizes: bit length of the modulus equal to 2048 or 3072 ⁷⁰ that meet the following: RSA PKCS#1 [R43] ⁷¹ or
---------------------	--

⁶⁴ [assignment: list of cryptographic operations]

⁶⁵ [selection: CMAC, Retail-MAC]

⁶⁶ [selection: 112, 128, 192, 256]

⁶⁷ [assignment: list of standards]

⁶⁸ [assignment: list of cryptographic operations]

⁶⁹ [assignment: list of cryptographic operations]

⁷⁰ [assignment: cryptographic key sizes]

⁷¹ [assignment: list of standards]

	<p>2. ECDSA with SHA-256 as specified in Table 6-4⁷² and cryptographic key sizes: 224 or 256 bit⁷³ that meet the following: FIPS 186-2 [R39]</p>
--	---

Table 6-3 RSA algorithms for signature verification in Terminal Authentication ([R13][R14])

Object Identifier	Signature	Hash	Parameters
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	Default

Table 6-4 ECDSA algorithms for signature verification in Terminal Authentication ([R13][R14])

Object Identifier	Signature	Hash
id-TA-ECDSA-SHA-256	ECDSA	SHA-256

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

Application Note 55 *For RSA and ECDSA cryptography the TOE makes use of the Infineon cryptographic library.*

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	<p>The TSF shall provide a mechanism to generate random numbers that meet BSI AIS-31 functionality class PTG.2 with strength of mechanism: high [R8]⁷⁴.</p>
-------------	---

⁷² [assignment: list of cryptographic operations]

⁷³ [assignment: cryptographic key sizes]

⁷⁴ [assignment: a defined quality metric]

--	--

Application Note 56 This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocols as required by FIA_UAU.4.

Application Note 57 The composite TOE makes use of the true random number generator (TRNG) of the IC M7892. The TRNG has already been evaluated as conformant to class PTG.2 of AIS-31 guidelines [R8] with strength of mechanism:high.

6.1.3 Class FIA Identification and Authentication

For the sake of better readability, Table 6-5 provides an overview of the authentication mechanisms used.

Table 6-5 Overview of authentication SFRs

Mechanism	SFR for the TOE	Comments
Authentication Mechanism for Initialization Agent	FIA_AFL.1/Init FIA_UAU.4	AES (256-bit keys)
Authentication Mechanism for Pre-personalization Agent and Personalization Agent	FIA_UAU.4 FIA_AFL.1/Pre-pers FIA_AFL.1/Pers	Triple-DES (112 bit keys) Retail MAC (112 bit keys)
Chip Authentication Protocol v.1	FIA_API.1/CAV1 FIA_UAU.5, FIA_UAU.6	Triple-DES (112 bit keys) AES (128, 192 and 256 bit keys) Retail MAC (112 bit keys) DH ECDH
Terminal Authentication Protocol v.1	FIA_UAU.5	RSASSA-PSS ECDSA
PACE protocol ⁷⁵	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE FIA_API.1/CAM	DH and ECDH with Integrated Mapping, Generic Mapping and Chip Authentication Mapping.
Passive Authentication	FIA_UAU.5/PACE	Verification of the hashes of DGs
Active Authentication	FIA_API.1/AA	RSA with SHA-256

⁷⁵ Only listed for information purposes

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

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

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

6.1.3.1 FIA_AFL.1 Authentication failure handling

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 ⁷⁶ unsuccessful authentication attempts occur related to <u>consecutive failed authentication attempts with respect to the initialization key</u> ⁷⁷ .
FIA_AFL.1.2/Init	When the defined number of consecutive unsuccessful authentication attempts has been <u>met</u> ⁷⁸ , the TSF shall <u>block the initialization key</u> ⁷⁹ .

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

⁷⁶ [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

⁷⁷ [assignment: list of authentication events]

⁷⁸ [assignment: met or surpassed]

⁷⁹ [assignment: list of actions]

FIA_AFL.1.1/Pre-pers	The TSF shall detect when <u>3</u> ⁸⁰ unsuccessful authentication attempts occur related to <u>consecutive failed authentication attempts with respect to the Pre-personalization key</u> ⁸¹ .
FIA_AFL.1.2/Pre-pers	When the defined number of consecutive unsuccessful authentication attempts has been <u>met</u> ⁸² , the TSF shall <u>block the Pre-personalization key</u> ⁸³ .

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 <u>an administrator configurable positive integer within the range between 1 and 15</u> ⁸⁴ unsuccessful authentication attempts occur related to <u>consecutive failed authentication attempts with respect to the Personalization key</u> ⁸⁵ .
FIA_AFL.1.2/Pers	When the defined number of consecutive unsuccessful authentication attempts has been <u>met</u> ⁸⁶ , the TSF shall <u>block the Personalization key</u> ⁸⁷ .

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

⁸⁰ [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

⁸¹ [assignment: list of authentication events]

⁸² [assignment: met or surpassed]

⁸³ [assignment: list of actions]

⁸⁴ [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

⁸⁵ [assignment: list of authentication events]

⁸⁶ [assignment: met or surpassed]

⁸⁷ [assignment: list of actions]

Hierarchical to: No other components.
 Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PACE	The TSF shall detect when <u>an administrator configurable positive integer within the range between 1 and 255</u> ⁸⁸ unsuccessful authentication attempts occur related to <u>consecutive failed authentication attempts with respect to the PACE password</u> ⁸⁹ .
FIA_AFL.1.2/PACE	When the defined number of consecutive unsuccessful authentication attempts has been <u>met</u> ⁹⁰ , the TSF shall <u>issue the result of the authentication with a few seconds delay</u> ⁹¹ .

Application Note 58 *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.*

6.1.3.2 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/PACE Timing of identification

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

FIA_UID.1.1/PACE	The TSF shall allow <ol style="list-style-type: none"> 1. <u>to establish the communication channel.</u> 2. <u>carrying out the PACE Protocol according to [R23].</u> 3. <u>to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS.</u>
------------------	---

⁸⁸ [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
⁸⁹ [assignment: list of authentication events]
⁹⁰ [assignment: met or surpassed]
⁹¹ [assignment: list of actions]

	<p>4. <u>to carry out the Chip Authentication Protocol v.1 according to [R13][R14]⁹²</u></p> <p>5. <u>to carry out the Terminal Authentication Protocol v.1 according to [R13][R14]⁹³</u></p> <p>6. <u>to carry out the Active Authentication Mechanism⁹⁴</u></p> <p>on behalf of the user to be performed before the user is identified.</p>
FIA_UID.1.2/PACE	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 59 *The SFR FIA_UID.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in the PACE PP [R12] by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 60 *After personalization in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization key).*

Application Note 61 *In the Step 5 “Initialization” of Phase 2 “Manufacturing of the TOE” the Initialization Agent is the only user role known to the TOE which writes the Initialization Data in the audit records of the IC. The user in role “Initialization Agent” identify himself by means of the GIM mechanism described in [R3]. In Step 6 “Pre-personalization” of Phase 2 “Manufacturing of the TOE” the Pre-personalization Agent is the only user role known to the TOE which writes the Pre-personalization Data in the audit records of the IC. The Pre-personalization Agent creates the user role Personalization Agent for transition from Phase 2 to Phase 3 “Personalization of the e-Document”. The users in role “Pre-personalization Agent” or “Personalization Agent” identify themselves by means of selecting the authentication key. After personalization in Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference*

⁹² [assignment: list of TSF-mediated actions]

⁹³ Only listed for information purposes

⁹⁴ [assignment: list of TSF-mediated actions]

Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalization Agent (using the Personalization key).

Application Note 62 User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the [e-Document](#) holder itself or an authorised other person or device (Basic Inspection System with PACE).

Application Note 63 In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalization Data in the audit records of the IC.

Please note that the Initialization Agent, or the Pre-personalization Agent or the Personalization Agent act on behalf of the [e-Document](#) Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Initialization Agent, Pre-personalization Agent and for Personalization Agent. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user roles “Initialization Agent”, “Pre-personalization Agent” or “Personalization Agent”, when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

6.1.3.3 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/PACE Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1/PACE	<p>The TSF shall allow</p> <ol style="list-style-type: none"> 1. <u>to establish the communication channel,</u> 2. <u>carrying out the PACE Protocol according to [R23],</u> 3. <u>to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,</u> 4. <u>to identify themselves by selection of the authentication key,</u>
------------------	--

	<p>5. <u>to carry out the Chip Authentication Protocol Version 1 according to [R13][R14]⁹⁵,</u></p> <p>6. <u>to carry out the Terminal Authentication Protocol Version 1 according to [R13][R14]⁹⁶,</u></p> <p>7. <u>to carry out the Active Authentication mechanism⁹⁷</u></p> <p>on behalf of the user to be performed before the user is authenticated.</p>
FIA_UAU.1.2/PACE	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 64 *The SFR FIA_UAU.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in the PACE PP [R12] by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.*

Application Note 65 *In the pre-operational phases of the TOE life cycle, the authentication key mentioned in point 4 of SFR FIA_UAU.1.1/PACE can be the Initialization key, the Pre-personalization key or the Personalization key.*

Application Note 66 *The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the e-Document holder itself or an authorised other person or device (BIS-PACE). If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}), cf. FTP_ITC.1/PACE.*

6.1.3.4 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).

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

Hierarchical to: No other components.

Dependencies: No dependencies.

⁹⁵ [assignment: list of TSF-mediated actions]

⁹⁶ [assignment: list of TSF-mediated actions]

⁹⁷ [assignment: list of TSF-mediated actions]

FIA_UAU.4.1	<p>The TSF shall prevent reuse of authentication data related to</p> <ol style="list-style-type: none"> 1. <u>PACE Protocol according to [R23]</u>. 2. <u>Authentication Mechanisms based on AES and Triple-DES⁹⁸,</u> 3. <u>Terminal Authentication Protocol v.1 according to [R13][R14]⁹⁹.</u>
-------------	--

Application Note 67 *The SFR FIA_UAU.4.1 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [R12].*

Application Note 68 *The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. In addition, the authentication of Pre-personalization Agent and of Personalization Agent makes use of a diversifier, thus ensuring protection against replay attacks, such as the use of an internal counter as a diversifier. Note that replay attacks have no effect in Initialization, as they can only repropose the same configuration data.*

6.1.3.5 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/PACE Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE	<p>The TSF shall provide</p> <ol style="list-style-type: none"> 1. <u>PACE Protocol according to [R23]</u>. 2. <u>Passive Authentication according to [R23]</u>. 3. <u>Secure messaging in MAC-ENC mode according to [R23]</u>.
------------------	--

⁹⁸ [selecion: Triple-DES, AES or other approved algorithms]

⁹⁹ [assignment: identified authentication mechanism(s)]

	<p>4. <u>Symmetric Authentication Mechanisms based on Triple-DES and AES</u>¹⁰⁰</p> <p>5. <u>Terminal Authentication Protocol v.1 according to [R13][R14]</u>¹⁰¹</p> <p>to support user authentication.</p>
<p>FIA_UAU.5.2/PACE</p>	<p>The TSF shall authenticate any user's claimed identity according to the following rules:</p> <ol style="list-style-type: none"> 1. <u>Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.</u> 2. <u>The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism based on Triple-DES with Personalization keys</u>¹⁰². 3. <u>After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v.1</u> <u>The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1</u>¹⁰³ Refinement: <u>or the public key presented during PACE-CAM and the secure messaging established by PACE-CAM .</u> 4. <u>The TOE accepts the authentication attempt as Initialization Agent by the Symmetric Authentication Mechanism based on AES with Initialization keys</u>¹⁰⁴. 5. <u>The TOE accepts the authentication attempt as Pre-personalization Agent by the Symmetric Authentication Mechanism based on Triple-DES with Pre-personalization keys</u>¹⁰⁵.

¹⁰⁰ [selection: *Triple-DES, AES or other approved algorithms*]

¹⁰¹ [assignment: *list of multiple authentication mechanism(s)*]

¹⁰² [selection: *the Authentication Mechanism with Personalization keys*]

¹⁰³ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

¹⁰⁴ [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

¹⁰⁵ [selection: *the Authentication Mechanism with Personalization keys*]

Application Note 69 *Please note that Passive Authentication does not authenticate any TOE's user, but provides evidence enabling an external entity (the terminal connected) to prove the origin of e-Document application.*

Application Note 70 *The Symmetric Authentication Mechanism for the Initialization Agent is based on AES and uses a diversification algorithm as described in [R3].*

Application Note 71 *The Symmetric Authentication Mechanism for Pre-personalization Agent and Personalization Agent uses the CPS protocol [R19] based on Triple-DES. This mechanism uses a key diversification algorithm based on data randomly chosen by the card.*

Application Note 72 *The PACE protocol may use both Triple-DES and AES to encipher the random generated in Step 1 of the protocol. However, usage of the algorithm Triple-DES is deprecated.*

Application Note 73 *The Embedded Software uses the symmetric co-processor provided by the platform to perform Triple-DES and AES.*

Application Note 74 *The SFR FIA_UAU.5.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.*

6.1.3.6 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/PACE Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions <u>each command sent to the TOE after successful run of the PACE Protocol shall be verified as being sent by the PACE terminal</u> ¹⁰⁶ .
------------------	---

Application Note 75 *The PACE protocol specified in [R23] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.*

FIA_UAU.6/EAC/CAV1 Re-authenticating – Re-authenticating of Terminal by the TOE after Chip Authentication version 1

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC/CAV1	The TSF shall re-authenticate the user under the conditions <u>each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System</u> ¹⁰⁷ .
----------------------	--

FIA_UAU.6/EAC/CAM Re-authenticating – Re-authenticating of Terminal by the TOE after PACE-CAM

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FIA_UAU.6.1/EAC/CAM	The TSF shall re-authenticate the user under the conditions <u>each command sent to the TOE after successful run of PACE with Chip Authentication Mapping shall be verified as being sent by the Inspection System</u> ¹⁰⁸ .
---------------------	---

Application Note 76 *The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [R23] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.*

6.1.3.7 FIA_API.1 Authentication Proof of Identity

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

FIA_API.1/CAV1 Authentication Proof of Identity by Chip Authentication Version 1

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/CAV1	The TSF shall provide a <u>Chip Authentication Protocol Version 1 according to [R23]</u> ¹⁰⁹ to prove the identity of the <u>TOE</u> ¹¹⁰ .
------------------	--

FIA_API.1/CAM Authentication Proof of Identity by PACE with Chip Authentication Mapping

Hierarchical to: No other components.

Dependencies: No dependencies.

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

¹⁰⁹ [assignment: authentication mechanism]

¹¹⁰ [assignment: authorized user or rule]

FIA_API.1.1/CAM	The TSF shall provide <u>PACE with Chip Authentication Mapping according to [R22]</u> ¹¹¹ to prove the identity of the <u>TOE</u> ¹¹² .
-----------------	---

Application Note 77 *This SFR requires the TOE to implement the Chip Authentication as either part of PACE-CAM specified in [R23] or as Chip Authentication Mechanism Version 1 specified in [R13][R14]. In the case of PACE-CAM the terminal verifies the authenticity of the chip using the Chip Authentication Data sent by the e-Document. In the case of Chip Authentication Version 1, the TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [R23]. the terminal verifies by means of secure messaging whether the e-Document’s chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication key (EF.DG14).*

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA	The TSF shall provide a <u>Active Authentication Protocol according to [R23]</u> ¹¹³ to prove the identity of the <u>TOE</u> ¹¹⁴ .
----------------	--

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/TRM Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

¹¹¹ [assignment: authentication mechanism]

¹¹² [assignment: authorized user or rule]

¹¹³ [assignment: authentication mechanism]

¹¹⁴ [assignment: authorized user or rule]

FDP_ACC.1.1/TRM	The TSF shall enforce the <u>Access Control SFP</u> ¹¹⁵ on <u>terminals gaining access to the User Data and data stored in EF.SOD of the logical e-Document</u> ¹¹⁶ .
-----------------	---

Application Note 78 The SFR FIA_ACC.1.1 in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by data stored in EF.SOD of the logical e-Document. This extension does not conflict with the strict conformance to PACE PP.

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM
 FMT_MSA.3 Static attribute initialization: not fulfilled, but justified

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

FDP_ACF.1.1 /TRM	The TSF shall enforce the <u>Access Control SFP</u> ¹¹⁷ to objects based on the following: 1. <u>Subjects</u> : a. <u>Terminal</u> , b. <u>BIS-PACE</u> , c. <u>Extended Inspection System</u> 2. <u>Objects</u> :
------------------	--

¹¹⁵ [assignment: access control SFP]

¹¹⁶ [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

¹¹⁷ [assignment: access control SFP]

	<ul style="list-style-type: none"> a. <u>data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical e-Document,</u> b. <u>data in EF.DG3 of the logical e-Document</u> c. <u>data in EF.DG4 of the logical e-Document</u> d. <u>all TOE intrinsic secret cryptographic keys stored in the e-Document¹¹⁸,</u> <p>3. <u>Security attributes:</u></p> <ul style="list-style-type: none"> a. <u>Authentication status of terminals</u> b. <u>PACE Authentication</u> c. <u>Terminal Authentication v.1,</u> d. <u>Authorisation of the Terminal¹¹⁹.</u>
<p>FDP_ACF.1.2/TRM</p>	<p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:</p> <ul style="list-style-type: none"> 1. <u>A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [R23] after a successful PACE authentication as required by FIA_UAU.1/PACE¹²⁰.</u>
<p>FDP_ACF.1.3/TRM</p>	<p>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none¹²¹.</u></p>
<p>FDP_ACF.1.4 /TRM</p>	<p>The TSF shall explicitly deny access of subjects to objects based on the following rules:</p> <ul style="list-style-type: none"> 1. <u>Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the e-Document</u> 2. <u>Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the e-Document</u> 3. <u>Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate</u>

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

¹¹⁹ [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

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

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

	<p><u>holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.</u></p> <p>4. <u>Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM</u></p> <p>5. <u>Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM</u></p> <p>6. <u>Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4¹²²</u></p>
--	---

Application Note 79 *The read access to user data in the personalization phase is protected by a Restricted Application Secret Code.*

Application Note 80 *The SFR FDP_ACF.1.1/TRM in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in this ST cover the definition in PACE PP [R12]. The SFR FDP_ACF.1.4/TRM in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by 3) to 6). These extensions do not conflict with the strict conformance to PACE PP.*

Application Note 81 *The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [R13][R14]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.*

Application Note 82 *Please note that the Document Security Object (SO_D) stored in EF.SOD (see [R22]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [R23].*

Application Note 83 *Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.*

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

6.1.4.3 FDP_RIP.1 Subset residual information protection

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

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1.1	<p>The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from¹²³ the following objects.</p> <ol style="list-style-type: none"> 1. <u>Session Keys (immediately after closing related communication session),</u> 2. <u>the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret K¹²⁴)¹²⁵</u>
-------------	---

6.1.4.4 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/TRM Basic data exchange confidentiality - e-Document

Hierarchical to: No other components.

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

¹²³ [selection: *allocation of the resource to, deallocation of the resource from*]

¹²⁴ According to [R23]

¹²⁵ [assignment: *list of objects*]

FDP_UCT.1.1/TRM	The TSF shall enforce the <u>Access Control SFP</u> ¹²⁶ to be able to <u>transmit and receive</u> ¹²⁷ user data in a manner protected from unauthorized disclosure.
-----------------	---

6.1.4.5 FDP_UIT.1 Basic 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/TRM Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1/TRM	The TSF shall enforce the <u>Access Control SFP</u> ¹²⁸ to be able to <u>transmit and receive</u> ¹²⁹ user data in a manner protected from <u>modification, deletion, insertion and replay</u> ¹³⁰ errors
FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> ¹³¹ has occurred.

Application Note 84 *FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes either after successful PACE-CAM or after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).*

¹²⁶ [assignment: access control SFP(s) and/or information flow control SFP(s)]

¹²⁷ [selection: transmit, receive]

¹²⁸ [assignment: access control SFP(s) and/or information flow control SFP(s)]

¹²⁹ [selection: transmit, receive]

¹³⁰ [selection: modification, deletion, insertion, replay]

¹³¹ [selection: modification, deletion, insertion, replay]

6.1.5 Class FTP Trusted Path/Channels

6.1.5.1 FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

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

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall enforce communication via the trusted channel for <u>any data exchange between the TOE and the Terminal</u> ¹³² .

Application Note 85 *The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word “initiate” is changed to ‘enforce’, as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.*

Application Note 86 *The trusted channel is established after successful performing the Chip Authentication protocol or the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{ENC}); If the Chip Authentication protocol was successfully performed, secure messaging is immediately restarted using the derived session keys. This secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE. Note that Terminal Authentication also requires secure messaging with the session keys established after Chip Authentication, either as part of PACE-CAM or as Chip Authentication Protocol Version 1.*

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

Application Note 87 *Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.*

FTP_ITC.1/CPS Inter-TSF trusted channel after CPS Authentication

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/CPS	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/CPS	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/CPS	The TSF shall enforce communication via the trusted channel for <u>any data exchange between the TOE and the Terminal in Pre-personalization and in Personalization</u> ¹³³ .

Application Note 88 *This SFR requires any data exchanged after a CPS authentication in Pre-personalization or in Personalization to be transmitted over a secured channel. In particular, Active Authentication data are transmitted through the secure channel established by the Pre-personalization Terminal.*

6.1.6 Class FMT Security Management

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

6.1.6.1 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.

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

Dependencies: No Dependencies

FMT_SMF.1.1	<p>The TSF shall be capable of performing the following security management functions:</p> <ol style="list-style-type: none"> 1. <u>Initialization</u>, 2. <u>Pre-Personalization</u>, 3. <u>Personalization</u>, 4. <u>Configuration</u>¹³⁴.
-------------	--

Application Note 89 *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 key may be used with uninitialized products only. Pre-personalization keys are only active in initialized products but not pre-personalized. Personalization keys are only active in pre-personalized but not personalized products. The e-Document locks out after a programmable number of consecutive unsuccessful authentication attempts. The Pre-personalization keys are disabled once pre-personalization is complete. The Personalization keys are disabled once personalization is complete.*

6.1.6.2 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/PACE Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1	<p>The TSF shall maintain the roles:</p> <ol style="list-style-type: none"> 1. <u>Manufacturer</u>, 2. <u>Personalization Agent</u>, 3. <u>Terminal</u>, 4. <u>PACE authenticated BIS-PACE</u>, 5. <u>Country Verifying Certification Authority</u>, 6. <u>Document Verifier</u>,
-------------	---

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

	<p>7. <u>Basic Inspection System</u>, 8. <u>Domestic Extended Inspection System</u>, 9. <u>Foreign Extended Inspection System</u>¹³⁵.</p>
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application Note 90 *The SFR FMT_SMR.1.1/PACE in this ST covers the definition in the EAC PP [R11] that, in turn, extends the definition in PACE PP [R12] by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.*

Application Note 91 *For explanation on the role Manufacturer and Personalization Agent please refer to the glossary. The role Terminal is the default role for any terminal being recognised by the TOE as not PACE authenticated BIS-PACE ('Terminal' is used by the e-Document presenter).*

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

Application Note 92 *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.*

6.1.6.3 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.

¹³⁵ [assignment: the authorised identified roles]

FMT_LIM.1.1	<p>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: <u>Deploying Test Features after TOE Delivery does not allow:</u></p> <ol style="list-style-type: none"> 1. <u>User Data to be disclosed or manipulated,</u> 2. <u>TSF data to be disclosed or manipulated,</u> 3. <u>software to be reconstructed,</u> 4. <u>substantial information about construction of TSF to be gathered which may enable other attacks and</u> 5. <u>sensitive User Data (EF.DG3 and EF.DG4) to be disclosed</u>¹³⁶.
-------------	--

6.1.6.4 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	<p>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: <u>Deploying Test Features after TOE Delivery does not allow:</u></p> <ol style="list-style-type: none"> 1. <u>User Data to be disclosed or manipulated,</u> 2. <u>TSF data to be disclosed or manipulated,</u> 3. <u>software to be reconstructed,</u> 4. <u>substantial information about construction of TSF to be gathered which may enable other attacks and</u> 5. <u>sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,</u>¹³⁷.
-------------	---

Application Note 93 *The formulation of “Deploying Test Features ...” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of*

¹³⁶ [assignment: limited capability and availability policy]

¹³⁷ [assignment: limited capability and availability policy]

FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

Note that the term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.1.6.5 FMT_MTD.1 Management of TSF data

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

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

FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to <u>write</u> ¹³⁸ the <u>Initialization Data and Pre-personalization Data</u> ¹³⁹ to the <u>Manufacturer</u> ¹⁴⁰ .
-------------------------	--

Application Note 95 *IC Initialization Data are written by the IC Manufacturer, TOE Initialization data are written by the Initialization Agent and Pre-personalization Data are written by the Pre-personalization Agent, according to the description given in section 1.5.2. The IC Initialization data include the Initialization key, the TOE Initialization Data include the Pre-personalization keys.*

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

Hierarchical to: No other components.

¹³⁸ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

¹³⁹ [assignment: *list of TSF data*]

¹⁴⁰ [assignment: *the authorised identified roles*]

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ INI_DIS	The TSF shall restrict the ability to <u>read out</u> ¹⁴¹ the <u>Initialization Data</u> and the <u>Pre-personalization Data</u> ¹⁴² to the <u>Personalization Agent</u> ¹⁴³
-------------------------	---

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_INI	The TSF shall restrict the ability to <u>write</u> ¹⁴⁴ the: <ol style="list-style-type: none"> 1. <u>initial Country Verifying Certification Authority Public Key,</u> 2. <u>initial Country Verifying Certification Authority Certificate,</u> 3. <u>initial Current Date</u>¹⁴⁵ to <u>the Personalization Agent</u> ¹⁴⁶ .
----------------------	---

Application Note 96 *The initial Country Verifying Certification Authority Public Key may be written by the Manufacturer in the production or pre-personalization phase or by the Personalization Agent (cf. [R13][R14]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.*

¹⁴¹ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

¹⁴² [assignment: *list of TSF data*]

¹⁴³ [assignment: *the authorised identified roles*]

¹⁴⁴ [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

¹⁴⁵ [assignment: *list of TSFdata*]

¹⁴⁶ [assignment: *the authorised identified roles*]

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/CVCA_UPD	<p>The TSF shall restrict the ability to <u>update</u>¹⁴⁷ the:</p> <ol style="list-style-type: none"> 1. <u>Country Verifying Certification Authority Public Key,</u> 2. <u>Country Verifying Certification Authority Certificate</u>¹⁴⁸, <p>to <u>Country Verifying Certification Authority</u>¹⁴⁹.</p>
----------------------	---

Application Note 97 *The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates (cf. [R13][R14]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [R13][R14]).*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/DATE	<p>The TSF shall restrict the ability to <u>modify</u>¹⁵⁰ the <u>Current Date</u>¹⁵¹ to:</p> <ol style="list-style-type: none"> 1. <u>Country Verifying Certification Authority,</u> 2. <u>Document Verifier,</u> 3. <u>Domestic Extended Inspection System</u>¹⁵²
------------------	--

¹⁴⁷ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

¹⁴⁸ [assignment: *list of TSF data*]

¹⁴⁹ [assignment: *the authorised identified roles*]

¹⁵⁰ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

¹⁵¹ [assignment: *list of TSF data*]

¹⁵² [assignment: *the authorised identified roles*]

Application Note 98 *The authorized roles are identified in their certificate (cf. [R13][R14]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication (cf. to [R13][R14]).*

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to <u>load</u> ¹⁵³ the <u>Chip Authentication Private Key</u> ¹⁵⁴ to <u>the Pre-personalization Agent</u> ¹⁵⁵
----------------------	---

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

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to <u>read</u> ¹⁵⁶ : <ol style="list-style-type: none"> 1. <u>PACE passwords,</u> 2. <u>Chip Authentication Private key,</u> 3. <u>Personalization keys.</u> 4. <u>Active Authentication Private Key,</u> 5. <u>Initialization key,</u> 6. <u>Pre-personalization keys</u>¹⁵⁷
-----------------------	---

¹⁵³ [selection: create, load]

¹⁵⁴ [assignment: list of TSF data]

¹⁵⁵ [assigned: the authorised identified roles]

¹⁵⁶ [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

¹⁵⁷ [assignment: list of TSF data]

	to <u>none</u> ¹⁵⁸ .
--	---------------------------------

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/ PA	The TSF shall restrict the ability to <u>write</u> ¹⁵⁹ the <u>Document Security Object (SO_D)</u> ¹⁶⁰ to the <u>Personalization Agent</u> ¹⁶¹ .
--------------------	--

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

¹⁵⁸ [assignment: *the authorised identified roles*]

¹⁵⁹ [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

¹⁶⁰ [assignment: *list of TSF data*]

¹⁶¹ [assignment: *the authorised identified roles*]

FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to <u>write</u> ¹⁶² the <u>Active Authentication Private Key</u> ¹⁶³ to <u>the Pre-personalization Agent</u> ¹⁶⁴ .
----------------------	--

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

6.1.6.6 FMT_MTD.3 Secure TSF data

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

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1	The TSF shall ensure that only secure values of the certificate chain are accepted for <u>TSF data of the Terminal Authentication Protocol v.1 and the Access Control</u> ¹⁶⁵ .
-------------	---

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

- 1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
- 2. the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE and the expiration date of Document Verifier Certificate is not before the Current date of the TOE,**
- 3. the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE.**

¹⁶² [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

¹⁶³ [assignment: *list of TSF data*]

¹⁶⁴ [assignment: *the authorised identified roles*]

¹⁶⁵ [assignment: *list of TSF data*]

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

Application Note 103 *The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.*

6.1.7 Class FPT Protection of the Security Functions

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

6.1.7.1 FPT_EMS.1 TOE emanation

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

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1	The TOE shall not emit electromagnetic and current emissions ¹⁶⁶ in excess of intelligible threshold ¹⁶⁷ enabling access to <ol style="list-style-type: none"> 1. <u>Chip Authentication session Keys,</u> 2. <u>PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),</u> 3. <u>the ephemeral private key ephem-SK_{PICC-PACE},</u>
-------------	---

¹⁶⁶ [assignment: type of emissions]

¹⁶⁷ [assignment: specified limits]

	<ol style="list-style-type: none"> 4. <u>Personalization keys,</u> 5. <u>Chip Authentication Private Key,</u> 6. <u>Active Authentication Private Key</u>¹⁶⁸, 7. <u>Initialization key,</u> 8. <u>Pre-personalization keys</u> and 9. <u>EF.DG1 to EF.DG16, EF.SOD, EF.COM</u>¹⁶⁹
FPT_EMS.1.2	<p>The TSF shall ensure <u>any users</u>¹⁷⁰ are unable to use the following interface <u>smart card circuits contacts</u>¹⁷¹ to gain access to</p> <ol style="list-style-type: none"> 1. <u>Chip Authentication session Keys,</u> 2. <u>PACE session Keys (PACE-K_{MAC}, PACE-K_{ENC}),</u> 3. <u>the ephemeral private key ephem-SK_{PICC-PACE},</u> 4. <u>Personalization keys,</u> 5. <u>Chip Authentication Private Key,</u> 6. <u>Initialization key,</u> 7. <u>Pre-personalization keys,</u> 8. <u>Active Authentication Private Key</u>¹⁷² and 9. <u>EF.DG1 to EF.DG16, EF.SOD, EF.COM</u>¹⁷³

Refinement:

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

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

Application Note 105 *The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation*

¹⁶⁸ [assignment: list of types of TSF data]

¹⁶⁹ [assignment: list of types of user data]

¹⁷⁰ [assignment: type of users]

¹⁷¹ [assignment: type of connection]

¹⁷² [assignment: list of types of TSF data]

¹⁷³ [assignment: list of types of user data]

of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The *e-Document's* chip can provide a smart card contactless interface according to ISO/IEC 14443 [R31][R32][R33][R34] and contact based interface according to ISO/IEC 7816-2 [R36] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

6.1.7.2 FPT_FLS Failure with preservation of secure state

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

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: <ol style="list-style-type: none"> 1. <u>Exposure to operating conditions causing a TOE malfunction,</u> 2. <u>Failure detected by TSF according to FPT_TST.1¹⁷⁴</u>
-------------	---

6.1.7.3 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.

¹⁷⁴ [assignment: *list of types of failures in the TSF*]

FPT_TST.1.1	The TSF shall run a suite of self tests <u>during initial start-up¹⁷⁵ , and at the conditions: before any use of TSF data¹⁷⁶</u> to demonstrate the correct operation of the TSF ¹⁷⁷ .
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of <u>the TSF data¹⁷⁸</u> .
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of <u>stored TSF executable code¹⁷⁹</u> .

Application Note 106 *A dedicated software in the protected ROM of the IC M7892 provides full test capabilities (operating system for test, “OST”), not accessible by the Security IC Embedded Software after delivery.*

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

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

6.1.7.4 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.

¹⁷⁵ [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*]]

¹⁷⁶ [assignment: *conditions under which self test should occur*]

¹⁷⁷ [selection: [assignment: *parts of TSF*], *the TSF*]

¹⁷⁸ [selection: [assignment: *parts of TSF*], *TSF data*]

¹⁷⁹ [selection: [assignment: *parts of TSF*], *TSF*]

FPT_PHP.3.1	The TSF shall resist <u>physical manipulation and physical probing</u> ¹⁸⁰ to the <u>TSF</u> ¹⁸¹ by responding automatically such that the SFRs are always enforced.
-------------	--

Application Note 109 *The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, ‘automatic response’ means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.*

6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

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

Table 6-6 Assurance requirements at EAL5+

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

Application Note 110 *The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications*

¹⁸⁰ [assignment: physical tampering scenarios]

¹⁸¹ [assignment: list of TSF devices/elements]

established using either PACE-CAM or the Chip Authentication Protocol v.1 (OE.Prot_Logical_e-Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).

6.3 Security Requirements Rationale

6.3.1 Security functional requirements rationale

Table 6-7 provides an overview for security functional requirements coverage of security objectives.

Table 6-7 Coverage of Security Objective for the TOE by SFR

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				X	X	X				X					
FCS_CKM.1/GIM				X			X								
FCS_CKM.1/CPS					X	X	X								
FCS_CKM.1/DH_PACE							X	X	X						
FCS_CKM.1/CA	X	X					X	X	X						
FCS_CKM.4	X				X	X	X	X	X						
FCS_COP.1/AUTH				X	X	X			X						
FCS_COP.1/AA_SIGN			X					X							
FCS_COP.1/PACE_ENC									X						
FCS_COP.1/CA_ENC	X	X		X	X	X	X		X						
FCS_COP.1/PACE_MAC							X	X							
FCS_COP.1/CA_MAC	X	X		X	X	X	X								
FCS_COP.1/SIG_VER	X														
FCS_RND.1	X				X	X	X	X	X						
FIA_AFL.1/Init													X		
FIA_AFL.1/Pre-pers													X		
FIA_AFL.1/Pers													X		
FIA_AFL.1/PACE													X		
FIA_UID.1/PACE	X		X	X	X	X	X	X	X						
FIA_UAU.1/PACE	X		X	X	X	X	X	X	X						
FIA_UAU.4/PACE	X			X	X	X	X	X	X						
FIA_UAU.5/PACE	X			X	X	X	X	X	X						
FIA_UAU.6/PACE							X	X	X						
FIA_UAU.6/EAC/CAV1	X						X	X	X						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Init	OT.AC_Pre-pers	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FIA_UAU.6/EAC/CAM	X						X	X	X						
FIA_API.1/CAV1		X													
FIA_API.1/CAM		X													
FIA_API.1/AA			X												
FDP_ACC.1/TRM	X			X	X	X	X		X						
FDP_ACF.1/TRM	X			X	X	X	X		X						
FDP_RIP.1							X	X	X						
FDP_UCT.1/TRM	X						X		X						
FDP_UIT.1/TRM							X		X						
FTP_ITC.1/PACE							X	X	X				X		
FTP_ITC.1/CPS							X	X	X						
FMT_SMF.1		X		X	X	X	X	X	X	X					
FMT_SMR.1/PACE		X		X	X	X	X	X	X	X					
FMT_LIM.1											X				
FMT_LIM.2											X				
FMT_MTD.1/INI_ENA				X	X	X				X					
FMT_MTD.1/INI_DIS						X				X					
FMT_MTD.1/CVCA_INI	X														
FMT_MTD.1/CVCA_UPD	X														
FMT_MTD.1/DATE	X														
FMT_MTD.1/CAPK	X	X					X								
FMT_MTD.1/PA						X	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X	X	X	X	X	X	X						
FMT_MTD.1/AAPK	X		X				X								
FMT_MTD.3	X														
FPT_EMS.1				X	X	X						X			
FPT_TST.1												X			X
FPT_FLS.1												X			X
FPT_PHP.3							X					X		X	

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

The security objective **OT.AC_Init** “Access Control for Initialization of logical **e-Document**” addresses the access control of the writing the logical **e-Document** in Step 5 “Initialization”. The Initialization Agent is authenticated by decrypting the initialization cryptograms using a mechanism based on AES as described in [R3] (FCS_COP.1/AUTH) with the Initialization key (FCS_CKM.1/GIM).

The authentication of the terminal as Initialization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Initialization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Initialization key, the TOE will use TSF according to the FCS_COP.1/CA_ENC (to verify the authentication attempt and for secure messaging) and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The session keys are destroyed according to FCS_CKM.4 after use.

The justification for the SFRs FAU_SAS.1, and FMT_MTD.1/INI_ENA arises from the justification for OT.Identification above with respect to the Initialization Data. The write access to the logical **e-Document** data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Initialization Agent is allowed to write the OS configuration data only once. The SFR FMT_SMR.1/PACE lists the roles (including Initialization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Initialization). The SFRs FMT_MTD.1/KEY_READ and FPT_EMS.1 restrict the access to the Initialization key.

The security objective **OT.AC_Pre-pers** “Access Control for Pre-personalization of logical **e-Document**” addresses the access control of the writing the logical **e-Document** in Step 6 “Pre-personalization”. The Pre-personalization Agent is authenticated by using the CPS mechanism based on Triple-DES (FCS_CKM.1/CPS, FCS_COP.1/AUTH and FCS_RND.1 [for key generation]) with the Pre-personalization keys by using the CPS mechanism.

The authentication of the terminal as Pre-personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Pre-personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Pre-personalization key, the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt and for secure messaging) and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The session keys are destroyed according to FCS_CKM.4 after use.

The justification for the SFRs FAU_SAS.1, and FMT_MTD.1/INI_ENA arises from the justification for OT.Identification above with respect to the Pre-personalization Data. The write access to the logical **e-Document** data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Pre-personalization Agent is allowed to write the data of the groups EF.DG14, EF.DG15 of the logical **e-Document** only once. The SFR FMT_SMR.1/PACE lists the roles (including Pre-personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Pre-personalization). The SFRs

FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalization keys, the Chip Authentication Private Key, PACE passwords and Active Authentication key.

The security objective **OT.AC_Pers** “Access Control for Personalization of logical **e-Document**” addresses the access control of the writing the logical **e-Document**. The Personalization Agent is authenticated by using the CPS mechanism based on Triple-DES (FCS_CKM.1/CPS, FCS_COP.1/AUTH and FCS_RND.1 [for key generation]), with the Personalization keys by using the CPS mechanism.

The justification for the SFRs FAU_SAS.1, FMT_MTD/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Personalization Data. The write access to the logical **e-Document** data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG13, EF.DG16 of the logical **e-Document** only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally, personalization data). The SFR FMT_SMR.1/PACE lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalization keys, the Chip Authentication Private Key, PACE passwords and Active Authentication key.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalization Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with the Personalization key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt and for secure messaging) and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging). The session keys are destroyed according to FCS_CKM.4 after use.

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

The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical **e-Document** stored on the **e-Document**’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Pre-personalization Agent or the Personalization Agent are allowed to write the data in EF.DG1 to EF.DG16 of the logical **e-Document** of the logical **e-Document** (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical **e-Document** (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy. The Personalization Agent must

identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. The Pre-personalization Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing data in Step 6 “Pre-personalization”. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, in Pre-personalization and Personalization by FTP_ITC.1/CPS, and in the Operational Use phase by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC for PACE. For secured data exchange in Initialization, a prerequisite is an authentication using an Initialization Key generated by the TOE (FCS_CKM.1/GIM). For secured data exchange in Pre-personalization and in Personalization, a prerequisite for establishing this trusted channel is a successful CPS Authentication using FCS_CKM.1/CPS. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

The TOE supports the inspection system detect any modification of the transmitted logical [e-Document](#) data after Chip Authentication v.1. The SFRs FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM and FDP_UIT.1/TRM require the integrity protection of the transmitted data after Chip Authentication performed either as part of PACE-CAM or as Chip Authentication Protocol v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

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

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication or Active Authentication) by enabling its verification at the terminal-side (PACE) and by an active verification by the TOE itself (PACE and Active Authentication).

This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC, as well as FTP_ITC.1/CPS. A prerequisite for establishing the trusted channel in the

Operational Use phase is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM. A prerequisite for establishing the trusted channel in Pre-personalization and in Personalization is a successful CPS authentication using FCS_CKM.1/CPS. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).

FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key.

FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered as trustworthy.

The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Data_Authenticity** is also achieved by FCS_COP.1/AA_SIGN.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.

This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC, as well as by FTP_ITC.1/CPS. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM. FDP_RIP.1 requires erasing the values of session keys (here: for K_{ENC}). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalization Agent only and, hence, is to be considered trustworthy.

The SFR FCS_RND.1 represents the general support for cryptographic operations needed.

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully

authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) performed as part of PACE-CAM or as Chip Authentication Protocol v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFRs FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM and FDP_UCT.1/TRM require the confidentiality protection of the transmitted data after Chip Authentication by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

The security objective **OT.Chip_Auth_Proof** "Proof of [e-Document's](#) chip authenticity" is ensured by the Chip Authentication provided by FIA_API.1/CAV1 and FIA_API.1/CAM proving the identity of the TOE. The Chip Authentication defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol performed as part of PACE-CAM [R23] or as Chip Authentication Protocol v.1 [R13][R14] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).

The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

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

The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by the 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_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

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

- i. while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;
- ii. for listening to PACE communication (is of importance for this ST, since SO_D is card-individual) – FTP_ITC.1/PACE.

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

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

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 6-8 shows the dependencies between the SFR of the TOE.

Table 6-8 Dependencies between the SFR for the TOE

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
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.1/CPS	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC Fulfilled by FCS_CKM.4,
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	<i>Justification 4 for non-satisfied dependencies</i> Fulfilled by FCS_CKM.4
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/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	<i>Justification 3 for non-satisfied dependencies</i> <i>Justification 3 for non-satisfied dependencies</i>
FCS_COP.1/AA_SIGN	[FDP_ITC.1 Import of user data without security attributes,	Fulfilled by FCS_ITC.1/PACE

	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 dependency
FCS_COP.1/PACE_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/DH_PACE Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/DH_PACE Fulfilled by FCS_CKM.4
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4 from [7]
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or	Fulfilled by FCS_CKM.1/CA,

	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4 from [7]
FCS_RND.1	No dependencies	-
FIA_AFL.1/Init	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/Pre-pers	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/Pers	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/PACE	No dependencies	n.a.
FIA_UAU.6/EAC/CAV1	No dependencies	n.a.
FIA_UAU.6/EAC/CAM	No dependencies	n.a.
FIA_API.1/CAV1	No dependencies	n.a.
FIA_API.1/CAM	No dependencies	n.a.
FIA_API.1/AA	No dependencies	n.a.
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM, justification 1 for non-satisfied dependencies
FDP_RIP.1	No dependencies	n.a.
FDP_UCT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel or	Fulfilled by FTP_ITC.1/PACE

	FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	n.a.
FTP_ITC.1/CPS	No dependencies	n.a.
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7]

		Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 from [7] Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

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

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

Justification 2: Since AA doesn't provide for generation or destruction of cryptographic keys, the SFR FCS_CKM.4 doesn't apply. The M7892 G12 platform provides for RSA cryptographic library functions.

Justification 3: 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 4: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

6.3.3 Security Assurance Requirements Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

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

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

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 depends on:

- ADV_ARC.1, Security architectural description
- ADV_FSP.4, Complete functional specification
- ADV_TDS.3, Basic modular design
- ADV_IMP.1, Implementation representation of the TSF
- AGD_OPE.1, Operational user guidance
- AGD_PRE.1, Preparative procedures
- ATE_DPT.1, Testing: basic design

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

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

All subjects and objects addressed by more than one SFR in section 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these "shared" items.

The assurance class EAL5 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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.AUTH_IDENT Identification & Authentication

This security service meets the following SFRs:

FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE,
FIA_UAU.6/PACE, FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM, FIA_AFL.1/Init,
FIA_AFL.1/Pre-pers, FIA_AFL.1/Pers, FIA_AFL.1/PACE, FCS_CKM.4, FIA_API.1/CAV1,
FIA_API.1/CAM, FIA_API.1/AA, FCS_COP.1/AA_SIG, FDP_RIP.1, FCS_CKM.1/GIM,
FCS_COP.1/AUTH

Access to functions and data of the TOE is only allowed to authenticated users. The authentication mechanism applied depends on the type of user system. Table 7-1 summarizes the authentication mechanisms for the various systems.

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 the 112-bit Pre-personalization keys
Personalization System	Initialized	CPS authentication based on Triple-DES with the 112-bit Personalization keys
Basic Inspection System – without PACE (BIS)	Operational	BAC based on Triple-DES with 112-bit Document Basic Access Keys.
Basic Inspection System supporting PACE (BIS-PACE)	Operational	PACE with either DH or ECDH key agreement. Generic Mapping, Integrated Mapping and Chip Authentication Mapping are supported.
Extended Inspection System not supporting PACE	Operational	BAC with Triple-DES algorithm with Document Basic Access Keys. Chip Authentication with either DH or ECDH key agreement Terminal Authentication with either RSA or ECDSA signature verification algorithms.
Extended Inspection System supporting PACE	Operational	PACE protocol with either DH or ECDH key agreement. Generic Mapping, Integrated Mapping and Chip Authentication Mapping are supported. Chip Authentication with either DH or ECDH key agreement Terminal Authentication with either RSA or ECDSA signature verification algorithms.

The Initialization Agent authenticates to the e-Document by decrypting the initialization cryptograms using the Initialization Key (FCS_CKM.1/GIM) using the algorithm described in [R3] based on AES with 256-bit keys (FCS_COP.1/AUTH). The Initialization Agent has only a limited number of authentication attempts after which the initialization commands are 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, sections 4.1, 5.2. [R19]. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and ICAO Doc 9303-11) (FCS_COP.1/AUTH) 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/PACE_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 (FIA_AFL.1/Pre-pers, FIA_AFL.1/Pers).

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/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE). 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 section 4.3 of the ICAO Doc 9303-11 [R23]) (FCS_COP.1/PACE_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/PACE_MAC). These authentication keys are derived by the SHA-1 algorithm (FIPS 180-4) as described in the ICAO Doc 9303-11, section 4.3 [R23].

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.

The PACE-enabled Basic Access System and the e-Document mutually authenticate by means of a PACE V2 protocol (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE). The e-Document and the Inspection System perform a Diffie-Hellman (DH or ECDH) key agreement by means of keys derived from a PACE password (MRZ, CAN or secret

password). After a successful authentication, the generated session keys are independent of PACE password entropy. 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 secure messaging encryption/decryption may be either a Triple-DES or AES (FCS_COP.1/PACE_ENC), the MAC algorithm may be a Retail MAC, coupled with Triple-DES encryption, or CMAC, coupled with AES encryption (FCS_COP.1/PACE_MAC).

After a successful PACE V2 authentication, the Inspection System is able to read less sensitive data, such as the MRZ, the facial image and other data easily available from other sources. If PACE-CAM has been performed, the authenticity of the chip has also been proved, thus allowing skipping of Chip Authentication Protocol v1.

If document inspection is performed on a Basic Inspection System, the e-Document's authenticity may also be proved executing the Active Authentication protocol. To this end, the TOE signs authentication data with the RSA algorithm with SHA-256 hashing (FCS_COP.1/AA_SIG, FIA_API.1/AA).

If document inspection is performed on a General Inspection System or an Extended Inspection System, then the e-Document's authenticity is proved executing the Chip Authentication Protocol v1 (as an alternative to PACE-CAM and Active Authentication). To this end two algorithms may be used: (i) a Diffie-Hellman key agreement compliant to PKCS #3 with key size 2048 bit or (ii) ECDH key agreement compliant to ISO15946 with key size up to 521 bit. Chip Authentication proves that the chip is genuine and also provides strong keys for Secure Messaging (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5, FIA_API.1/CAV1, FIA_API.1/CAM, FCS_CKM.1/CA).

If document inspection is performed on an Extended Inspection System, then after a successful Chip Authentication the e-Document's chip recognizes that the Inspection System is entitled to access sensitive data, such as fingerprints, iris image and other data not easily available from other sources by means of the Terminal Authentication protocol (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FCS_COP.1/SIG_VER). Terminal Authentication attempts are only accepted after a successful Chip Authentication performed either as part of PACE-CAM or as Chip Authentication Protocol Version 1 and a consequent restart of the Secure Messaging session with the strong keys computed in the Chip Authentication.

The combination of Chip Authentication and Terminal Authentication provides an implementation of the Extended Access Control mechanism.

7.1.2 SS.SEC_MSG Secure data exchange

This security service meets the following SFRs:

FCS_CKM.1/CPS, FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC,

FCS_COP.1/AUTH, FCS_CKM.4, FIA_UAU.6/PACE, FIA_UAU.6/EAC/CAV1, FIA_UAU.6/EAC/CAM, FDP_RIP.1

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 (Triple-DES and AES 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 may either be:

- Triple-DES [R41] in CBC mode with key size 112 bits (FIPS 46-3 and ICAO Doc 9303-11), with message authentication code computed according to Retail MAC algorithm and cryptographic key size 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).
- AES [R42] in CBC mode with key sizes 128, 192 and 256 bits, with message authentication code computed according to [R40] with MAC length of 8 bytes.

The session keys are calculated during the authentication phase (FCS_CKM.1/DH_PACE, FCS_CKM.1/CA). If a PACE or Chip Authentication protocol is executed, then the Secure Messaging is restarted using the session keys computed during that authentication. The channel will be closed in case of a received message with:

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

After a PACE or Chip Authentication protocol has been completed, the TOE rejects those commands that cause a failure of Secure Messaging (FIA_UAU.6/PACE). Session keys are overwritten with zeroes after usage (FCS_CKM.4).

7.1.3 SS.ACC_CNTRL Storage and Access Control of Data Objects

This security service meets the following SFRs:

FDP_ACC.1/TRM, FDP_ACF.1/TRM, FAU_SAS.1, FDP_UCT.1/TRM, FDP_UIT.1/TRM, FMT_SMF.1, FMT_SMR.1/PACE, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FTP_ITC.1/PACE, FTP_ITC.1/CPS, FMT_MTD.1/PA, FMT_MTD.1/AAPK, FDP_RIP.1

As required in FDP_ACF.1/TRM, 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 TOE identification data, the DF LDS and the Initialization key are written during the IC manufacturing by the IC Manufacturer.

The OS configuration parameters and the Pre-personalization keys are written during initialization by the Initialization Agent.

The Chip Authentication key pair (public key in DG14), the Active Authentication key pair (public key in DG15), the symmetric keys for the authentication of the Personalization Agent, the document number, the application serial number, the Application Restricted Secret Code, the EF.CardAccess and the Security Environment object are written during the pre-personalization phase by the Pre-personalization Agent.

The Document Basic Access Keys, the current date, the CVCA public key, the trustpoint, the EF.CVCA, the Document Number, the PACE key 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. In the operational phase access to initialization and pre-personalization data is denied.

7.1.4 SS.LFC_MNG Life cycle management

This security service meets the following SFRs:

FMT_SMF.1, FMT_SMR.1/PACE

It ensures that the TOE life cycle status is set in an irreversible way to mark the transition to the operational use status. The only role allowed to set the life cycle status is the Personalization Agent.

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 are 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_EMS.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 chip already certified; a more detailed formulation of the security functions provided by the chip can be found in the security target of the IC [R26].

7.1.7 SS.SIG_VER Verification of digital signatures

This security service meets the following SFRs:

Terminal Autentication

FCS_COP.1/SIG_VER, FMT_SMR.1/PACE, FMT_MTD.1/CVCA_INI,
FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.3

The signatures to be verified are based on (i) RSA according to PKCS#1 [R43] with key sizes of 2048 or 3072 bit or (ii) ECDSA with key sizes of 224 or 256 bit (FCS_COP.1/SIG_VER).

The signature verification is performed through the check of the certificate chain up to a trusted start point (a public key of the Country Verifying Certificate Authority, see FMT_MTD.3) and the current date handling (cf. [BSI, 2.2.4]). Once a signature is recognized as valid then security roles can be maintained according to FMT_SMR.1 and the CVCA certificate and the current date can be updated (FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE).

The validity of the certificate chain is proven at the TOE current date if and only if:

- i. the digital signature of the Inspection System Certificate, checked using the public key of the Document Verifier Certificate, is recognized as valid and the Inspection System Certificate is not expired
- ii. the digital signature of the Document Verifier Certificate, checked using the public key in the Certificate of the Country Verifying Certification Authority, is recognized as valid and the Document Verifier Certificate is not expired
- iii. the digital signature of the Certificate of the Country Verifying Certification Authority, checked using its own public key, is recognized as valid and certificate of the Country Verifying Certification Authority is not expired

Active Authentication

FCS_COP.1/AA_SIGN

The Inspection system can have a proof of the TOE identity by verifying signatures based on the algorithm RSA with SHA-256 and cryptographic key sizes 2048 and 3072 bits that meet the following the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital Signature scheme 1

[R29].

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

Table 7-2 Coverage of SFRs by security services

	SS.AUTH_IDENT 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	SS.SIG_VER Verification of digital signatures
FAU_SAS.1			X				
FCS_CKM.1/GIM	X						
FCS_CKM.1/CPS		X					
FCS_CKM.1/DH_PACE		X					
FCS_CKM.1/CA		X					
FCS_CKM.4	X	X					
FCS_COP.1/PACE_ENC		X					
FCS_COP.1/PACE_MAC		X					
FCS_COP.1/CA_ENC		X					
FCS_COP.1/CA_MAC		X					
FCS_COP.1/SIG_VER							X
FCS_COP.1/AA_SIG	X						X
FCS_COP.1/AUTH	X	X					
FCS_RND.1						X	
FIA_AFL.1/Init	X						
FIA_AFL.1/Pre-pers	X						
FIA_AFL.1/Pers	X						
FIA_AFL.1/PACE	X						
FIA_UID.1/PACE	X						
FIA_UAU.1/PACE	X						
FIA_UAU.4/PACE	X						
FIA_UAU.5/PACE	X						
FIA_UAU.6/EAC/CAV1	X	X					
FIA_UAU.6/EAC/CAM	X	X					
FIA_UAU.6/PACE	X	X					
FIA_API.1/CAV1	X						
FIA_API.1/CAM	X						
FIA_API.1/AA	X						
FDP_ACC.1/TRM			X				
FDP_ACF.1/TRM			X				
FDP_UCT.1/TRM			X				

FDP_UIT.1/TRM			X				
FDP_RIP.1	X	X	X				
FTP_ITC.1/PACE		X					
FTP_ITC.1/CPS		X					
FMT_SMF.1			X	X			
FMT_SMR.1/PACE			X	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/CVCA_INI			X				X
FMT_MTD.1/CVCA_UPD			X				X
FMT_MTD.1/DATE			X				X
FMT_MTD.1/CAPK			X				
FMT_MTD.1/KEY_READ			X				
FMT_MTD.1/PA			X				
FMT_MTD.1/AAPK			X				
FMT_MTD.3							X
FPT_EMS.1						X	
FPT_FLS.1						X	
FPT_TST.1					X	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 semi-formal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements. These documents, together with the source code of the software, address the ADV_ARC, ADV_FSP, ADV_TDS and ADV_IMP families.

The configuration management plan addresses the ALC_CMC and ALC_CMS families and enforces good practices to securely manage configuration items including, but not limiting to, design documentation, user documentation, source code, test documentation and test data.

The configuration management process guarantees the separation of the development configuration libraries from the configuration library containing the releases and also supports the generation of the TOE.

All the configuration items are managed with the help of automated tools. In particular configuration items regarding security flaws are managed with the support of an issue tracking system, while all the other configuration items are managed with the help of a version control system.

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

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

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

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

The life-cycle model adopted in the manufacturing phases and the tools supporting the development and production of the TOE are described in a dedicated document addressing the assurance family ALC_LCD.

Tools and techniques adopted in the development process are documented, thus addressing the assurance family ALC_TAT.

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

Due to the composite nature of the evaluation, which is based on the CC evaluation of the hardware, the assurance measures related to the platform (IC) are covered by documents from the IC manufacturer. The security recommendations 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	Documentation
ADV_ARC.1	Description of the Security Architecture of the SOMA-c007 embedded software
ADV_FSP.5	Functional Specification for the SOMA-c007 embedded software
ADV_IMP.1	Source code of the SOMA-c007 embedded software
ADV_INT.2	Rationale of the quality characteristics of SOMA-c007 embedded software.
ADV_TDS.4	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.5	Configuration Management Plan, configuration list evidences of configuration management
ALC_DEL.1	Secure Delivery procedure Delivery documentation
ALC_DVS.2	Development security description Development security documentation
ALC_LCD.1	Life-cycle definition
ALC_TAT.2	Tools and techniques definition
ATE_COV.2	Coverage of Test Analysis for the SOMA-c007 Electronic Document
ATE_DPT.3	Depth of Test Analysis for the SOMA-c007 Electronic Document
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.5	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 9303-10)
CPS	Common Personalization Standard
CPU	Central Processing Unit
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DF	Dedicated File (ISO 7816)
DG	Data Group (ICAO Doc 9303-10)
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
ECB	Electronic Codebook (block cipher mode of operation)
EEPROM	Electrically Erasable Read Only Memory
EF	Elementary File (ISO 7816)
EIS	Extended Inspection System
ESW	Embedded Software
GIM	Generic Initialization Mechanism
GIS	General Inspection System
IC	Integrated Circuit
IS	Inspection System
LDS	Logical Data Security
LCS	Life Cycle Status
MAC	Message Authentication Code
MF	Master File (ISO 7816)
MMU	Memory Management Unit
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
N/A	Not Applicable
n.a.	Not Applicable
OCR	Optical Character Recognition
OS	Operating System
OSP	Organization Security Policy
PACE	Password Authenticated Connection Establishment
PACE-GM	PACE with Generic Mapping
PACE-IM	PACE with Integrated Mapping

PACE-CAM	PACE with Chip Authentication Mapping
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
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
SSCD	Secure Signature Creation Device
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

<i>Active Authentication</i>	Security mechanism defined in ICAO Doc 9303-11 [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.
<i>application note</i>	Additional information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
<i>audit records</i>	Write-only-once non-volatile memory area of the e-Documents chip to store the Initialization Data and Pre-personalization Data.
<i>authenticity</i>	Ability to confirm the e-Document and its data elements on the e-Document’s chip were created by the Issuing State or Organization.
<i>Basic Access Control</i>	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.
<i>Basic Inspection System</i>	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.
<i>biographical data</i>	The personalized details of the bearer of the document appearing as text in the Visual Inspection Zone (VIZ) and Machine Readable Zone (MRZ) on the biographical data page of a document book or card [R22].
<i>biometric reference data</i>	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.
<i>Certificate chain</i>	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).
<i>Chip Authentication</i>	Authentication protocol used to verify the genuinity of the e-Document chip.
<i>counterfeit</i>	An unauthorized copy or reproduction of a genuine security document made by whatever means.
<i>Country Signing Certification Authority (CSCA)</i>	Certification Authority of the Issuing State or Organization which attests the validity of certificates and digital signatures issued by the Document Signer.
<i>Country Signing Certification Authority Certificate (C_{CSCA})</i>	Certificate of the Country Signing Certification Authority Public Key (PK _{CSCA}) issued by Country Signing Certification Authority stored in the inspection system.
<i>Country Verifying Certification Authority (CVCA)</i>	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.
<i>Current Date</i>	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.
<i>CVCA link Certificate</i>	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.

<i>Document Basic Access Keys</i>	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 document book to authenticate an entity able to read the printed MRZ of the document book.
<i>Document Security Object</i>	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}) [R23].
<i>Document Signer</i>	Entity delegated by the Issuing State or Organization to digitally sign the DG's present in the LDS.
<i>eavesdropper</i>	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.
<i>e-Document</i>	A document or other official document of identity issued by a State or organization, which may be used by the rightful holder.
<i>e-Document application</i>	Non-executable data defining the functionality of the operating system on the IC as the e-Document's chip. It includes: <ul style="list-style-type: none"> 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.DG14 and EF.DG 16) and iii. the TSF Data including the definition the authentication data but except the authentication data itself.
<i>e-Document Basic Access Control</i>	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.
<i>e-Document holder</i>	The rightful holder of the e-Document for whom the issuing State or Organization personalized the e-Document.
<i>e-Document's chip</i>	An integrated circuit chip complying with ISO/IEC 14443 (contactless interface) and/or ISO/IEC 7816-2 (contact interface) and programmed according to the LDS [R22].
<i>e-Document's chip Embedded Software</i>	Software embedded in an 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.
<i>enrolment</i>	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].
<i>Extended Access Control</i>	Security mechanism identified in BSI TR-03110 [R13][R14] 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.
<i>Extended Inspection System</i>	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.
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [R22].
<i>General Inspection System</i>	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
<i>Global interoperability</i>	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.
<i>IC Initialization Data</i>	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.
<i>impostor</i>	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.
<i>Initialization Agent</i>	The agent who initializes the e-Document by writing Initialization Data.
<i>Initialization Data</i>	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).
<i>Inspection</i>	The act of a State examining an e-Document presented to it by a user (the e-Document holder) and verifying its authenticity.
<i>Inspection System</i>	A technical system used by the border control officer of the receiving State (i) examining an e-Document presented by the user and verifying its authenticity and (ii) verifying the user as e-Document holder.
<i>Integrated Circuit</i>	Electronic component(s) designed to perform processing and/or memory functions. The e-Document's chip is an integrated circuit.
<i>integrity</i>	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
<i>Issuing Organization</i>	Organization authorized to issue an official e-Document (e.g. the United Nations Organization, issuer of the document).
<i>Issuing State</i>	The Country issuing the e-Document.
<i>Logical Data Structure</i>	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.

<p><i>Logical e-Document</i></p>	<p>Data of the e-Document holder stored according to the LDS [R23] as specified by ICAO on the IC. It presents contact or contactless readable data including (but not limited to):</p> <ul style="list-style-type: none"> 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).
<p><i>Machine Readable Electronic Document</i></p>	<p>Official document issued by a State or Organization which is used by the holder for various purposes (e.g. travel document, 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 [R16] [R23].</p>
<p><i>Machine Readable Zone</i></p>	<p>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].</p>
<p><i>machine-verifiable biometrics feature</i></p>	<p>A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a e-Document in a form that can be read and verified by machine.</p>
<p><i>Optional biometric reference data</i></p>	<p>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.</p>
<p><i>Passive Authentication</i></p>	<p>Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by:</p> <ul style="list-style-type: none"> 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.
<p><i>Personalization</i></p>	<p>The process by which the portrait, signature and biographical data are applied to the document [R22].</p>

<i>Personalization Agent</i>	The agent delegated by the Issuing State or Organization to personalize the e-Document for the holder by <ol style="list-style-type: none"> 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.
<i>Personalization Agent Authentication Information</i>	TSF data used for authentication proof and verification of the Personalization Agent.
<i>Physical e-Document</i>	e-Document in the form of paper, plastic and chip using secure printing to present data including (but not limited to): <ol style="list-style-type: none"> i. biographical data, ii. data of the MRZ, iii. photographic image and iv. other data.
<i>Pre-personalization Agent</i>	The agent who performs pre-personalization by writing Pre-personalization Data.
<i>Pre-personalization Data</i>	Any data that is injected into the non-volatile memory of the TOE by the Pre-personalization Agent (Phase 2) for traceability of non-personalized e-Documents and/or 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.
<i>Pre-personalized Document's chip</i>	e-Document's chip equipped with a unique identifier, the Personalization keys, and a unique asymmetric Active Authentication Key Pair of the chip.
<i>presenter</i>	A person presenting the e-Document to the inspection system and claiming the identity of the e-Document holder.
<i>Primary Inspection System</i>	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.
<i>Receiving State</i>	The Country to which the e-Document holder is applying for entry [R24].
<i>reference data</i>	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.
<i>secure messaging</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R23].

<i>skimming</i>	Imitation of the inspection system to read the logical e-Document or parts of it via the contact or contactless communication channel of the TOE without knowledge of the printed MRZ data.
<i>TOE Initialization Data</i>	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2) in Step 5 Initialization.
<i>TSF data</i>	Data created by and for the TOE, that might affect the operation of the TOE [R16].
<i>Unpersonalized e-Document</i>	e-Document material prepared to produce an personalized e-Document containing an initialized and pre-personalized e-Document's chip.
<i>User data</i>	Data created by and for the user, that does not affect the operation of the TSF [R16].
<i>Verification</i>	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 [R23].
<i>Verification data</i>	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, Basic Access Control, ref. TCAE160001.*
- [R2] **Arjo Systems:** *Security Target SOMA-c007 Machine Readable Electronic Document, Secure Signature Generation, 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] **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*
- [R8] **BSI:** *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*
- [R9] **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*
- [R10] **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.*
- [R11] **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.*

- [R12] **BSI:** *Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.01, 22nd July 2014, BSI-CC-PP-0068-V2-2011-MA-01.*
- [R13] **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*
- [R14] **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*
- [R15] **BSI:** *Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17 April 2012*
- [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, June 2003*
- [R20] **European Parliament:** *Directive 1999/93/EC on a "Community framework for electronic signatures"*
- [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] **ICAO:** *Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015, Part*

12: Public Key Infrastructure for MRTDs

- [R25] **Infineon:** *M7892 Controller Family for Security Applications, Hardware Reference Manual, revision 1.3 2013-03-11*
- [R26] **Infineon:** *Public Security Target M7892 Design Steps D11 and G12, revision 1.7 as of 2016-11-12*
- [R27] **IETF Network Working Group:** *Request For Comments 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997.*
- [R28] **ISO/IEC:** *International Standard 7816-4 2005 Information Technology – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange – January 15, 2005*
- [R29] **ISO/IEC:** *International Standard 9796-2:2002 Information Technology – Security Techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanism, Second edition 2002-10-01*
- [R30] **ISO/IEC:** *International Standard 9797-1 1999 Information Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*
- [R31] **ISO/IEC:** *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics.*
- [R32] **ISO/IEC:** *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface.*
- [R33] **ISO/IEC:** *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision.*
- [R34] **ISO/IEC:** *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol.*
- [R35] **ISO/IEC:** *International Standard 10116:2006 – Information technology – Security techniques – Modes of operation for a n-bit block cipher, third edition 2006-02-01*
- [R36] **ISO/IEC:** *International Standard 7816-2:2007 Identification cards - Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts*
- [R37] **JIWG:** *Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, version 1.4, August 2015*

- [R38] **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*
- [R39] **NIST:** *Federal Information Processing Standards Publication FIPS PUB 186-2, DIGITAL SIGNATURE STANDARD (DSS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, January 2000*
- [R40] **NIST:** *Special publication 800-38B, Recommendation for block cipher modes of operation, The CMAC mode for authentication, 2005*
- [R41] **NIST:** *Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), 1999*
- [R42] **NIST:** *Federal Information Processing Standards Publication FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001*
- [R43] **RSA Laboratories:** *PKCS#1 – RSA cryptography standard, An RSA Laboratories Technical Note, version 2.1 June 2002.*
- [R44] **RSA Laboratories:** *PKCS #3 - Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, version 1.4 November 1993.*
- [R45] **RSA Laboratories:** *PKCS #15 v1.1: Cryptographic Token Information Syntax Standard*
- [R46] **Arjo Systems:** *Secure Delivery Procedure, ref. TCAE110027*
- [R47] **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. [R37]), 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. [R7]), 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. [R26]).

END OF DOCUMENT