ID&TRUST

IDENTITY APPLET V3.4-P1/PACE-EAC1/AA

EPASSPORT WITH PACE-GM, PACE-CAM, EXTENDED ACCESS CONTROL V1 AND ACTIVE AUTHENTICATION

SECURITY TARGET

COMMON CRITERIA / ISO 15408

EAL4+

2021

Classification: Public

Revision history

Version	Date	Information
V1.00	18.08.2020	Final version
V1.01	13.10.2020	Update references Minor modification in section 1.4.2
V1.02	04.06.2021	Update TOE identification data
V1.03	16.06.2021	Update TOE name and ST title
V1.04	28.06.2021	Update section 1.1, 1.4 and Bibliography

Table of Contents

List of Tables

1 ST Introduction

1 This section provides document management and overview information that are required a potential user of the TOE to determine, whether the TOE fulfils her requirements.

2 Throughout this document, the term PACE refers to PACE v2, and the term EAC refers to EAC 1.

3 The ICAO Technical Report "Supplemental Access Control" [14] describes how to migrate from the current access control mechanism, Basic Access Control, to PACE v2, a new cryptographically strong access control mechanism that is initially provided supplementary to Basic Access Control:

4 "There is no straightforward way to strengthen Basic Access Control as its limitations are inherent to the design of the protocol based on symmetric (“secret key”) cryptography. A cryptographically strong access control mechanism must (additionally) use asymmetric (“public key”) cryptography.

5 The ICAO Technical Report "Supplemental Access Control” [14] specifies PACE as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic Access Control, i.e.

- Since 1st January 2018 states may implement PACE without implementing Basic Access Control.
- Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.

6 Note that Basic Access Control will remain the “default” access control mechanism for globally interoperable machine readable travel documents as long as Basic Access Control provides sufficient security. Basic Access Control may however become deprecated in the future. In this case PACE will become the default access control mechanism.

7 The inspection system SHALL use either BAC or PACE but not both in the same session."

8 Within the migration period, some developers will have to implement their products to functionally support both, PACE and Basic Access Control (BAC), i.e. Supplemental Access Control (SAC). However, any product using BAC will not be conformant to the current ST; i.e. a product implementing the TOE may functionally use BAC, but, while performing BAC, they are acting outside of security policy defined by the current ST. Therefore, organizations being responsible for the operation of inspection systems shall be aware of this context.

9 The TOE is a composite TOE. The Common Criteria Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices [8] contains all the relevant information about the methodology to handle such a TOE. The developer followed the direction of the mandatory document, and so should any relevant parties participate in the evaluation and certification of the TOE.

1.1 ST Reference

10	Title:	IDentity Applet v3.4-p1/PACE-EAC1/AA – ePassport with PACE-GM, PACE-CAM, Extended Access Control v1 and Active Authentication
	Author:	ID&Trust Ltd.
	Version Number:	1.04
	Date:	28.06.2021

1.2 TOE Reference

11 The Security Target refers to the product “ID&Trust IDentity Applet Suite v3.4” for CC evaluation.

12	TOE Name:	IDentity Applet v3.4-p1/PACE-EAC1 on NXP JCOP 4 P71
13	TOE short name:	IDentity Applet v3.4/PACE-EAC1/AA
14	TOE Identification Data:	
	Applet version number	IDentity Applet V3.4/PACE-EAC1/AA v3.4.7470
	Patch version number:	015A
15	Evaluation Criteria:	[4]
16	Evaluation Assurance Level:	EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
17	Developer:	ID&Trust Ltd.
18	Evaluation Sponsor:	NXP Semiconductors Netherlands B.V. 5656, AG Eindhoven, High Tech Campus 60

1.3 TOE Overview

1.3.1 TOE definition

19 The TOE comprises:

I. Underlying platform of the TOE, which is evaluated by Brightsight and certified by TÜV Rheinland Nederland B.V. at assurance level

Evaluation assurance level:	EAL6 augmented by ASE_TSS.2 and ALC_FLR.1.
CC Certification number:	NSCIB-CC-180212-CR3
Long platform name:	JCOP 4 P71
Short name:	JCOP 4

It consists of:

- Micro Controller (a secure smart card controller from NXP from the SmartMX3 family);
- IC Dedicated Software (MC FW Micro Controller Firmware and Crypto Library);
- IC Embedded Software JCOP4 (Java Card Virtual Machine, Runtime Environment, Java Card API;
- Global Platform (GP) Framework;

II. the Application Part of the TOE:

ID&Trust IDentity Applet Suite v3.4/PACE-EAC1;

III. the associated guidance documentation [5],[6].

20 **1. Application note (from ST author)**

The EAC PP [17] refers to the TOE as MRTD, Machine Readable Travel Documents or Travel Document. In order to facilitate the better usage the terminology is not changed in the current ST.

1.3.2 TOE usage and major security features

21 The Target of Evaluation (TOE) addressed by the current Security Target is an electronic travel document representing a contact or contactless smart card programmed according to ICAO Technical Report “Supplemental Access Control” [14] (which means amongst others according to the Logical Data Structure (LDS) defined in [13]) and additionally providing the Extended Access Control (EAC) according to the ‘ICAO Doc 9303’ [13] and BSI TR-03110 [9], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE [18] and PACE-Chip Authentication Mapping, which enables much faster authentication of the of the chip than running PACE with General Mapping followed by CA.

22 IDentity Applet Suite v3.4 is a highly configurable eID solution. It is able to satisfy multiple different application requirements even within a single applet instance. The Application part of the TOE, the applet functionalities are distributed according to the following table:

Application	Function	Standard	Protection Profile (certified or in progress)
IDentity/PKI	Flexible PKI token	CEN TS 14890-1/2 IAS-ECC 1.0.1 [23]	-
IDentity/IAS	European card for e-Services and National e-ID applications	CEN/TS 15480-2 [22] IAS-ECC 1.0.1 [23]	-
IDentity/QSCD	Qualified Signature Creation Device	CEN/TS 15480-2 [22] IAS-ECC 1.0.1[23] REGULATION (EU) No 910/2014 [24]	[19] [20]
IDentity/IDL	International Driving License	ISO/IEC 18013	-
IDentity/EDL	European Driving License	2012/383/EC	-
IDentity/eVR	Electronic Vehicle Registration	1999/37/EC	-
IDentity/eHC	Electronic Health Insurance	CEN/CWA 15794	-
IDentity/BAC	Basic Access Control (BAC)	ICAO Doc 9303 [13]	BSI-CC-PP-0055 [16]
IDentity-J	Basic Access Control (BAC) Password Authenticated Connection Establishment (PACE)	ICAO Doc 9303 [13]	JISEC500 [29] JISEC499 [30]
IDentity/PACE-EAC1	Password Authenticated Connection Establishment (PACE) (GM and PACE-CAM) Extended Access Control v1 (EAC1)	ICAO Doc 9303 [13] ICAO TR-SAC [14] BSI TR-03110 v2.21 [9], [10], [11], [12]	BSI-CC-PP-0068-V2-2011 [18] BSI-CC-PP-0056-V2-2012 [17]
IDentity/eIDAS	Password Authenticated Connection Establishment (PACE) Extended Access Control v2 (EAC2)	ICAO TR-SAC [14] BSI TR-03110 v2.21 [9], [10], [11], [12]	BSI-CC-PP-0087 [21]

1. Table IDentity Applet Suite v3.4 functionalities

23 All the functions are supplied by the applet “IDentity Applet Suite v3.4”, the behaviour of the applet changes according to the configuration applied during the personalization phase and the environmental behaviour of the usage phase.

The scope of the current ST is only concerned with applet behaviour of configuration IDentity Applet 3.4/PACE-EAC1/AA.

24 This Security Target defines the security objectives and requirements for the contact based / contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment with Generic Mapping (PACE-GM) and Chip Authentication Mapping (PACE-CAM), Extended Access Control, and Chip Authentication similar to the Active Authentication in ‘ICAO Doc 9303’ [13].

25 If the product is using the BAC-established communication channel (see TOE documentation) it will not be conformant to the claimed (section 2.2) PPs of [18] and [17] i.e. the product implementing the TOE may functionally use BAC, but, while performing BAC, it is acting outside of security policy defined by the PPs [17], [18].

26 For the TOE, beside the IDentity Applet 3.4/PACE-EAC1/AA application other applications may be present on the Platform. Other applications are not relevant for the current ST and do not infer the Security Functions of the TOE. The TOE utilises the evaluation of the underlying Platform.

27 Part of the TOE is the associated guidance documentation, the IDentity Applet Suite v3.4 Administrator’s Guide [5] and IDentity Applet Suite v3.4 User’s Guide [6].

28 The intended customer of the product the Card Issuer, who is in charge of the issuance of the product to the smartcard holders.

1.3.3 TOE Type

29 The TOE is the Smart Card Integrated Circuit with Dedicated Software, Embedded Software and IDentity Applet v3.4/PACE-EAC1/AA.

1.3.4 Non-TOE hardware/software/firmware

30 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 inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE

1.4 TOE Description

1.4.1 Product type

31 The TOE is the Smart Card Integrated Circuit with Dedicated Software, Embedded Software and IDentity Applet v3.4/PACE-EAC1/AA, viewed as unit of

i. the physical part of the travel document in form of paper and/or plastic and chip. It presents visual readable data including (but not limited to) personal data of the travel document holder
   a) the biographical data on the biographical data page of the travel document surface,
   b) the printed data in the Machine Readable Zone (MRZ) and
   c) the printed portrait.

32 ii. the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [13] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder
   a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
   b) the digitized portraits (EF.DG2),
   c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both
   d) the other data according to LDS (EF.DG5 to EF.DG16) and
   e) the Document Security Object (SOD).

33 **2. Application note (from the ST author)**

The biometric reference data (EF.DG3 and EF.DG4) are optional according to [13]. If the issuing State or Organisation uses this option it should protect these data by means of Extended Access Control (EAC1). It means that the TOE can operate with PACE complying to this ST, the use of EAC is conditional to the use of EF.DG3 and/or EF.DG4.

1.4.2 Components of the TOE

34 **Micro Controller**

The Micro Controller is a secure smart card controller from NXP from the SmartMX3 family. The Micro Controller contains a co-processor for symmetric cipher, supporting DES operations and AES, as well as an accelerator for asymmetric algorithms. The Micro Controller further contains a physical random number generator. The supported memory technologies are volatile (Random Access Memory (RAM)) and non-volatile (Read Only Memory (ROM) and FLASH) memory. Access to all memory types is controlled by a Memory Management Unit (MMU) which allows to separate and restrict access to parts of the memory.

IC dedicated software – Micro Controller Firmware

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices and for writing data to non-volatile memory.

IC dedicated software – Crypto Library

The Crypto Library provides implementations for symmetric and asymmetric cryptographic operations, hashing, the generation of hybrid deterministic and hybrid physical random numbers and further tools like secure copy and compare. The supported asymmetric cryptographic operations are ECC and RSA. These algorithms use the Public Key Crypto Coprocessor (PKCC) of the Micro Controller for the cryptographic operations.

Micro Controller, IC dedicated software (Micro Controller Firmware, Crypto Library) are covered by the following certification: Certification ID: BSI-DSZ-CC-1136-2021

Evaluation level EAL6+ ALC_FLR.1 and ASE_TSS.2 according to Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-00084-2014.

Embedded Software

Certification ID:	NSCIB-CC-180212-CR3

JCOP4 consists of Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Global Platform (GP) framework, Configuration Module, etc.

OS Name:	JCOP 4 Operating System
Applied OS configuration:	Banking & Secure ID
Product Identification:	JCOP 4 v4.7 R1.01.4
Evaluation Level:	CC EAL 6+ with ASE_TSS.2, ALC_FLR.1 according to Java Card System – Open Configuration Protection Profile, version 3.0.5, Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI, BSI-CC-PP-0099-2017).
Platform UGD:	[27]

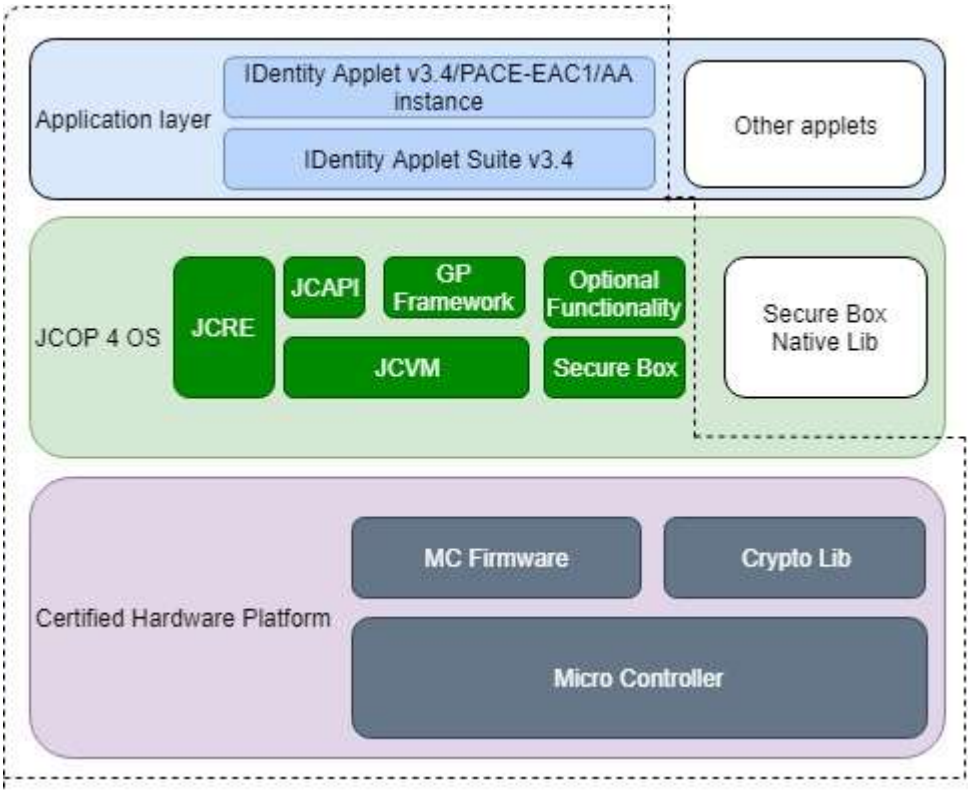
IDentity Applet – accomplishing IDentity application

Product name:	ID&Trust IDentity Applet Suite
Version:	3.4
Applet name[1]:	IDentity Applet V3.4/PACE-EAC1/AA ePassport with PACE, EAC1 and Active Authentication
TOE Guidance	
Documentation[2]:	IDentity Applet Suite v3.4 Administrator's Guide [5]
	IDentity Applet Suite v3.4 User's Guide [6]
Version:	3.4

The composite part always means IDentity Applet v3.4/PACE-EAC1/AA

35 The logical architecture of the TOE:

[1] The applet is provided in cap file format.
[2] The AGD documents provided in electronic document format.



1. Figure TOE Boundaries

36 The TOE is a composite TOE and the dashed line denotes the whole TOE. The underlying certified hardware platform and JCOP 4 OS are marked with purple and green. In this ST the common short name of certified hardware platform and JCOP 4 OS is Platform.

The blue box marks the application layer. The ID&Trust IDentity Applet Suite v3.4 could be loaded in the Flash. During the creation phase an instance is created in the Flash and after several configuration steps it will be personalized as IDentity Applet v3.4/PACE-EAC1/AA. For details please see: section 1.4.4 TOE life cycle and [5].

The boxes marked with white are not certified.

1.4.3 TOE usage and security features for operational use

37 The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

38 The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [13]. These security measures can include the binding of the travel document's chip to the travel document.

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

40 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [13], and Password Authenticated Connection Establishment (with Generic Mapping (PACE-GM) and

Chip Authentication Mapping (PACE-CAM)) [14]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

41 This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This Security Target addresses the Chip Authentication Version 1 described in [9] as an alternative to the Active Authentication stated in [13] and PACE-CAM [14].

42 If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [16] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

43 The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)' [18]. Note that [18] considers high attack potential.

44 For the PACE protocol according to [14], the following steps shall be performed:

i. the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.
ii. The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
iii. The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.
iv. Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [9], [14].

45 The security target requires the TOE to implement - among others - the Extended Access Control as defined in [9]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data (EF.DG3 and/or EF.DG4) during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of

(i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and
(ii) (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems.

The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates. The Active Authentication enables to the inspection system to verify that the TOE chip is genuine, based on a static key pair (Active Authentication Key Pair) stored in the chip.

1.4.4 TOE life cycle

46 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [15], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

47 **3. Application note (from the ST author)**

The IDentity Applet Life cycle has the following phases, which differ from the whole TOE Lifecycle:

- IDentity Applet

LOADED (Creation phase)

- IDentity Instance

Personalization Phase

SELECTABLE (Configuration Phase)

CONFIGURED (Initialization Phase)

Operational Phase

PERSONALIZED

LOCKED

BLOCKED

These phases are detailed in the ID&Trust IDentity Applet Suite Administrator's Guide [5]. These states and phases are presented here, because of informational reasons, to serve better understanding.

48 **Phase 1 of TOE life-cycle "Development"**

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software (i.e. Crypto Library) and the guidance documentation associated with these TOE components.

49 (Step2) IC developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system). The IDentity Applet v3.4/PACE-EAC1/AA application and the corresponding guidance documentation are developed by ID&Trust Ltd.[3]

50 The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software and the IDentity Applet v3.4/PACE-EAC1/AA in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. Part of the IC Embedded Software is in the non-volatile non-programmable memories, and the guidance documentation is securely delivered to the travel document manufacturer.

51 **4. Application note (from the ST author)**

The delivery procedures between ID&Trust (applet developer) and the manufacturer:

1. The IDentity Applet Developer develops a new version of the ID&Trust IDentity Applet v3.4/PACE-EAC1/AA.
2. After the new version is tested a new release is issued and stored in configuration management system.
3. The new version of the IDentity Applet v3.4/PACE-EAC1/AA is sent to as required by [28].

[3] In the case of the current Security Target, the Software Developers are two separated entities, NXP and ID&Trust. While NXP has developed the Common Criteria Certified Platform, the IC Embedded Software (Operating System) and the IC Dedicated Software (cryptographic library), IDentity Applet 3.4/PACE-EAC1/AA implementing the eMRTD functionality is developed by ID&Trust.

52 **Phase 2 of TOE life cycle "Manufacturing"**

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (ROM) and the IDentity Applet Suite v3.4 in FLASH. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacture to the travel document manufacturer.

53 (Step4 optional) The travel document manufacturer combines the IC with hardware for the contact based/contactless interface in the travel document.

54 (Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD's chips with pre-personalization data.

55 **5. Application note (redefined for the goals of this ST by the ST author, taken from Application note 1 from [17])**

Creation of the application implies that the Creation Phase of the IDentity Applet 3.4/PACE-EAC1/AA is closed, and the it gets to SELECTABLE state (Configuration Phase). Further details are discussed within the IDentity Applet Administrator's Guide [5].

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

The Personalization Agent Authentication Keys are the preinstalled keys for the IDentity Applet, which are preinstalled by the Travel Document Manufacturer, and which are needed and used in the Personalization process.

56 **Phase 3 of TOE life-cycle "Personalisation of the travel document"**

(Step6) The personalisation of the travel document includes:

(i) the survey of the travel document holder's biographical data,
(ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
(iii) the printing of the visual readable data onto the physical part of the travel document,
(iv) the writing of the TOE User Data and TSF Data into the logical travel document and
(v) configuration of the TSF if necessary.

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

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

57 **6. Application note (from the ST author)**

The Personalisation Phase of the IDentity Applet contains the Configuration and Initialisation Phase.
During Configuration phase all applications, files, security data objects, configuration variables, file and object parameters are created. Specified settings in the configuration phase fundamentally determine the Application Profile, which is protected by the Application Profile Signature.

In the **Initialisation Phase** the content of the IDentity Applet instance is loaded. The signing of the Document Security Object by the Document Signer is crucial in this phase since the signature of the Document Security Object supports to verify genuineness of the MRTD's chip (DG.14 with Chip Authentication v1 or DG.15 with Active Authentication).

The referred Personalization Agent can be the Card Issuer, or a different contributor on the Card Issuer discretion.

These phases are detailed in the ID&Trust IDentity Applet Suite Administrator's Guide [5]. These states and phases are presented here for informational reasons, to serve better understanding.

7. Application note (taken from application note 2 from [17])

58 The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] § 92) comprise (but are not limited to) the Personalization Agent Authentication Key(s) the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

59 **Phase 4 of the TOE life-cycle "Operational Use"**

(Step7) The TOE is used as a travel document's chip by the traveller 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.

8. Application note (taken from application note 4 from [17])

The intention of the ST is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet 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.

60 Note that the personalisation 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, the Security Target has to outline the split up of P.Manufact, P.Personalisation and the related security objectives into aspects relevant before vs. after TOE delivery.

61 Some production steps, e.g. Step 4 in Phase 2 (Manufacturing) may also take place in the Phase 3 (Personalisation of the travel document).

1.4.5 TOE security functions

62 The following TOE ensured security functions are the most significant for its operational use:

63
- Only entities (e.g. terminals) possessing authorisation can get access to the user data stored on the TOE and use security functionality of the travel document under control of the travel document holder,

64
- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the entity connected,

65
- Averting of inconspicuous tracing of the travel document,

66
- Self-protection of the TOE security functionality and the data stored inside.

67 Above mentioned functions are described below informally, and in detail in section 7.1.

1.4.6 Features of the IDentity Applet Suite v3.4

68 This section is informational and intended to provide a general detail about the IDentity Applet Suite v3.4 which is the essential part of this ST. Information in this section does not extend the TOE description or claims of this ST.

69 IDentity Applet Suite v3.4 may be considered as a highly secure and configurable multi-application cryptographic smart card framework for PKI and e-ID purposes.

70 IDentity Applet Suite v3.4 complies with the standards referenced in TOE Overview.

71 The API exposed by IDentity Applet Suite v3.4 allows fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and Payment applications.

72 IDentity Applet Suite v3.4 is designed for the Java Card family of smart card platforms and specifically for the NXP JCOP IC which is certified according to the CC EAL 6+ both the Micro Controller, Crypto Library and the JCOP 4 as well. The Platform is protected against state of the art attacks.

73 The Platform provides:

- Cryptographic algorithms and functionality (3DES, AES, RSA, SHA, ECC, RNG, DH, etc.);
- GlobalPlatform 2.3 functionality;
- Three different communication protocol (ISO 7816 T=1, T=2, ISO 14443 T=CL (contact-less);
- Java Card 3.0.5 functionality (secure memory management, garbage collection, extended Length APDUs, etc.)
- NXP Proprietary functionality (Secure Box, Secure Messaging Accelerator Interface, JAVA CARD API for data encryption via PUF).

2 Conformance Claims

2.1 Conformance with the Common Criteria

74 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation (CC),

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

as follows

- Part 2 extended, (see Chapter 5 Extended components definition)
- Part 3 conformant.

75 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]

has to be taken into account.

2.2 Protection Profile Claim

76 The current ST claims strict conformance to the following Protection Profiles:

Title	**Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP)**
Sponsor	Bundesamt für Sicherheit in der Informationstechnik
CC Version	3.1 (revision 3)
Assurance Level	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
General Status	Final
Version number	version 1.3.2
Registration	BSI-CC-PP-0056-V2-2012
Keywords	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)
Title	**Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP)**
Sponsor	Bundesamt für Sicherheit in der Informationstechnik
CC Version	3.1 (revision 4)
Assurance Level	EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
General Status	Final
Version number	Version 1.01
Registration	BSI-CC-PP-0068-V2-2011-MA-01
Keywords	ePassport, travel document, ICAO, PACE, Standard Inspection Procedure, Supplemental Access Control (SAC)

2.3 Package Claim

77 The current ST is conformant to assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in the CC, part 3 [3].

2.4 Conformance rationale

78 The ST is built on the PP-s referenced above, which according to the certifications conform to the CC version stated above.

79 This ST is conformant with Common Criteria Part 2 [2] extended due to additional components as stated in Protection Profiles: [17] and [18].

80 This ST is conformant to Common Criteria Part 3 [3].

81 The current ST refines the assets, threats, objectives and SFRs of [17] and [18].

82 The Security Target claims **strict conformance** to two PPs:

- Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2 BSI-CC-PP-0056-V2-2012. [17]
- Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01 Version 1.01, 22th July 2014 [18]

83 The Target of Evaluation (TOE) addressed by the current Security Target is an electronic travel document representing a contactless / contact smart card programmed according to ICAO Technical Report "Supplemental Access Control" [14].

The TOE is thus **consistent** with the **TOE type** in the PPs:

BSI-CC-PP-0056-V2-2012 [17]:

The protection profile defines the security objectives and requirements for the contact based / contactless smart card of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organization (ICAO).

BSI-CC-PP-0068-V2-2011-MA-01 [18]:

The TOE type is contactless/contact smart card with the *ePassport* application named as a whole 'travel document'.

84 The **security problem definition** of this security target is **consistent** with the statement of the security problem definition in the PPs, as the security target claims strict conformance to the PPs and no other threats.

85 The **security objectives for the TOE** of this security target are **consistent** with the statement of the security objectives in the PPs as the security target claims strict conformance to the PPs. There are two security objectives added, **OT.Active_Auth_Proof** (Proof of travel document's chip authenticity) and **OT.Chip_Auth_Proof_PACE_CAM** (Proof of the electronic document's chip authenticity).

Justification: OT.Active_Auth_Proof was added because the Active Authentication, OT.Chip_Auth_Proof_PACE_CAM because the Chip Authentication mapping, both of them are optional functions of TOE.

These security objectives do not affect the strict conformance.

86 The **security objectives for the operational environment** in this security target include all security objectives for the operational environment from the PPs. There is one objective added, **OE.Active_Auth_Key_Travel_Document** (Travel document Active Authentication Key).

Justification: OE.Active_Auth_Key_Travel_Document was added because of the Active Authentication, the optional function of TOE.

This security objective does not affect the strict conformance.

87 The **security requirements** of this security target are **consistent** with the statement of the security requirements in the PPs as the security target claims strict conformance to the PPs.

The following SFR was iterated because of FMT_MTD.1/CAPK:

- FCS_CKM.1/CA_GEN

The following SFRs were iterated because of PACE-CAM:

- FCS_CKM.1/CAM
- FCS_COP.1/CAM
- FIA_API.1/PACE-CAM

The following SFR was extended to the ST because of PACE-CAM:

- FPT_EMS.1

The following SFRs were refined to the ST because of PACE-CAM:

- FIA_UID.1/PACE
- FIA_UAU.5/PACE

The following SFRs were iterated because the Active Authentication protocol:

- FCS_CKM.1/AA_GEN
- FCS_COP.1/EMRTD
- FIA_API.1/AA
- FMT_MTD.1/AAPK

The following SFRs was extended to the ST because of Active Authentication protocol:

- FPT_EMS.1

The following SFRs were refined to the ST because of Active Authentication protocol:

- FIA_UAU.4/PACE
- FMT_MTD.1/KEY_READ

There are the following SFRs iterated from [2]

- FCS_CKM.1/AA_GEN
- FCS_CKM.1/CA_GEN
- FCS_COP.1/EMRTD
- FMT_MTD.1/AAPK
- FCS_CKM.1/CAM
- FCS_COP.1/CAM

There are the following SFRs iterated from sec. 5:

- FIA_API.1/AA
- FIA_API.1/PACE-CAM

There are the following SFRs extended:

- FPT_EMS.1

There are the following SFRs refined:

- FIA_UID.1/PACE
- FIA_UAU.4/PACE
- FIA_UAU.5/PACE
- FMT_MTD.1/KEY_READ

Justification: The iterations and extensions of above mentioned SFRs were necessary because Active Authentication and PACE – Chip Authentication mapping, the optional functions of TOE.

These additional SFRs do not affect the strict conformance. All assignments and selections of the security functional requirements defined in the [17] and [18] are done accordingly.

2.5 Statement of compatibility

2.5.1 Security Functionalities

88 The following table contains the security functionalities of the Platform ST [7] and of current ST, showing which Functionality correspond to the Platform ST and which has no correspondence. This statement is compliant to the requirements of [8].

89 A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as 'relevant' or 'not relevant' for current ST

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant/Not relevant	Remarks
SF.JCVM	TSF.Platform	Relevant	Java Card Virtual Machine
SF.CONFIG	TSF.Platform	Relevant	Configuration Management
SF.OPEN	TSF.AccessControl TSF.Authenticate TSF.Platform	Relevant	Card Content Management
SF.CRYPTO	TSF.AppletParametersSign TSF.Authenticate TSF.CryptoKey TSF.Platform	Relevant	Cryptographic Functionality
SF.RNG	TSF.CryptoKey TSF.Platform	Relevant	Random Number Generator
SF.DATA_STORAGE	TSF.AppletParametersSign TSF.CryptoKey TSF.Platform	Relevant	Secure Data Storage
SF.PUF	-	Not relevant	User Data Protection using PUF
SF.EXT_MEM	-	Not relevant	External Memory
SF.OM	TSF.Platform	Relevant	Java Object Management
SF.MM	-	Not relevant	Memory Management
SF.PIN	TSF.AppletParametersSign	Relevant	PIN Management
SF.PERS_MEM	TSF.Platform	Relevant	Persistent Memory Management
SF.SENS_RES	-	Not relevant	Sensitive Result
SF.EDC	TSF.Platform	Relevant	Error Detection Code API
SF.HW_EXC	TSF.Platform	Relevant	Hardware Exception Handling
SF.RM	-	Not relevant	Restricted Mode
SF.PID	-	Not relevant	Platform Identification
SF.SMG_NSC	TSF.Platform	Relevant	No Side-Channel
SF.ACC_SBX	-	Not relevant	Secure Box
SF.MOD_INVOC	-	Not relevant	Module Invocation

2. Table Classification of Platform-TSFs

90 All the above Platform TSFs which are indicated as relevant are relevant for this ST.

91 **9. Application note (from the ST author)**

The TSF.Platform Security functionality in the above list represents functionalities which are not directly used in IDentity Applet, they are implicitly invoked by calls to the Platform, respectively the JCOP 4. These functions are called altogether as TSF.Platform.

2.5.2 Organisational Security Policies (OSPs)

92 P.Card_PKI, P.Trustworthy_PKI, P.Terminal, P.Sensitive_Data and P.Personalisation are not applicable to the Platform and therefore not mappable for [7].

93 The OSP.VERIFICATION, OSP.PROCESS-TOE, OSP.KEY-CHANGE are covered by the ALC class, furthermore P.Manufact and P.Pre-Operational correspond to these OSPs.

94 OSP.SECURE-BOX and OSP.SECURITY-DOMAINS do not deal with any additional security components.

95 OSP.SECURE-BOX and OSP.SECURITY-DOMAINS do not deal with any additional security components.

2.5.3 Security objectives

96 The following Platform-ST objectives can be mapped to this STs objectives as shown in the following table, so they are relevant.

Objective from the Platform-ST	Objective from this ST
OT.ALARM	OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.CARD-CONFIGURATION	OT.Prot_Abuse-Func
OT.CARD-MANAGEMENT	OT.AC_Pers OT.AC_Pers OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf
OT.CIPHER	OT.AC_Pers OT.Active_Auth_Proof OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Sens_Data_Conf
OT.COMM_AUTH	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf OT.Tracing
OT.COMM_CONFIDENTIALITY	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf OT.Tracing
OT.COMM_INTEGRITY	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf OT.Tracing
OT.COMM-AUTH	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf OT.Tracing
OT.DOMAIN-RIGHTS	OT.AC_Pers OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Identification OT.Sens_Data_Conf
OT.GLOBAL_ARRAYS_CONFID	OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity
OT.IDENTIFICATION	OT.AC_Pers OT.Identification

Objective from the Platform-ST	Objective from this ST
OT.KEY-MNGT	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Sens_Data_Conf OT.Tracing
OT.OPERATE	OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Malfunction OT.Prot_Phys-Tamper
OT.PIN-MNGT	OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Malfunction
OT.REALLOCATION	OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity
OT.RESOURCES	OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.RND	OT.AC_Pers OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Sens_Data_Conf
OT.RNG	OT.AC_Pers OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Sens_Data_Conf
OT.SCP.IC	OT.AC_Pers OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.SCP.RECOVERY	OT.Data_Integrity OT.Prot_Inf_Leak OT.Prot_Phys-Tamper
OT.SCP.SUPPORT	OT.AC_Pers OT.Chip_Auth_Proof OT.Chip_Auth_Proof_PACE_CAM OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity OT.Sens_Data_Conf OT.Tracing
OT.SID_MODULE	OT.Prot_Inf_Leak OT.Prot_Malfunction
OT.TRANSACTION	OT.Data_Authenticity OT.Data_Confidentiality OT.Data_Integrity

3. Table Mapping of security objectives for the TOE

97 The following Platform-ST objectives are not relevant for or cannot be mapped to the TOE of this ST:

- **OT.SID**
- **OT.APPLI-AUTH**
- **OT.ATTACK-COUNTER**
- **OT.EXT-MEM**
- **OT.FIREWALL**
- **OT.Global_ARRAYS_INTEG**
- **OT.NATIVE**
- **OT.OBJ-DELETION**
- **OT.RESTRICTED-MODE**

- **OT.SEC_BOX_FW**
- **OT.SENSITIVE_RESULT_INTEG**

cannot be mapped because these are out of scope.

98 The objectives for the operational environment can be mapped as follows:

Objective from the Platform-ST	Classification of OE	Objective from this ST
OE.APPLET	CfPOE	Covered by ALC class
OE.PROCESS_SEC_IC	CfPOE	Covered by the Platform's certification and ALC class
OE.VERIFICATION	CfPOE	Covered by ALC class
OE.CODE-EVIDENCE	CfPOE	Covered by ALC class
OE.USE_DIAG	SgOE	Covered by OE.Terminal, OE.Exam_Travel_Document and OE. OE.Prot_Logical_Travel_Document
OE.USE_KEYS	SgOE	Covered by OE.Terminal, OE.Exam_Travel_Document and OE.Prot_Logical_Travel_Document
OE.APPS-PROVIDER	CfPOE	Covered by ALC class
OE.VERIFICATION-AUTHORITY	CfPOE	Covered by ALC class
OE.KEY-CHANGE	CfPOE	Covered by ALC class
OE.SECURITY-DOMAINS	CfPOE	Covered by ALC class

4. Table Mapping of security objectives of the environment

99 There is no conflict between security objectives of this ST and the Platform-ST.

2.5.4 Security requirements

100 The Security Requirements of the Platform-ST can be mapped as follows:

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
FAU_ARP.1	FPT_PHP.3	RP_SFR-MECH	FAU_ARP.1 facilitate to protect the TOE as required by FPT_PHP.3.
FAU_SAS.1[SCP]	FAU_SAS.1	RP_SFR-MECH	FAU_SAS.1[SCP] covers the requirement of FAU_SAS.1
FCO_NRO.2[SC]	-	IP_SFR	-
FCS_CKM.1t	FCS_CKM.1/CA_GEN	RP_SFR-SERV	FCS_CKM.1.1 of the Platform is applied to generate the static CA key pair.
	FCS_CKM.1/AA_GEN	RP_SFR-SERV	FCS_CKM.1.1 of the Platform is applied to generate the Active Authentication key pair.
FCS_CKM.4	FCS_CKM.4-	RP_SFR-MECH	FCS_CKM.4 of the Platform covers FCS_CKM.4
FCS_COP.1	FCS_CKM.1/CAM	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement during the PACE-CAM.
	FCS_CKM.1/DH_PACE	RP_SFR-SERV	FCS_COP.1.1[ECDHPACEKeyAgreement] is applied for key agreement during the PACE protocol.

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
			FCS_COP1.1[SHA] is applied for session key derivation during PACE protocol.
	FCS_COP.1/PACE_ENC	RP_SFR-SERV	FCS_COP.1.1[TripleDES] or FCS_COP.1.1[AES] is applied for nonce encryption during the PACE protocol. FCS_COP.1.1[TripleDES] or FCS_COP.1.1[AES] is applied for encryption during the secure messaging.
	FCS_COP.1/CAM	RP_SFR-SERV	FCS_COP1.1[AES] is applied for nonce encryption during the PACE-CAM protocol. FCS_COP1.1[AES] is applied for encryption and decryption during secure messaging (PACE-CAM)
	FCS_CKM.1/CA	RP_SFR-SERV	FCS_COP.1.1[SHA] is applied for session key derivation during Chip Authentication version 1. FCS_COP.1.1[ECDH_P1363] is applied during the Chip authentication version 1 for session key agreement. FCS_COP1.1[SHA] is applied for session key derivation during PACE-CAM protocol.
	FCS_COP.1/PACE_ENC	RP_SFR-SERV	FCS_COP.1.1[TripleDES] or FCS_COP.1.1[AES] is applied for message encryption and decryption during PACE secure messaging.
	FCS_COP.1/CA_ENC	RP_SFR-SERV	FCS_COP.1.1[TripleDES] or FCS_COP.1.1[AES] is applied for message encryption and decryption during CA secure messaging.
	FCS_COP.1/PACE_MAC	RP_SFR-SERV	FCS_COP.1.1[AESMAC] or FCS_COP.1.1[DESMAC] is applied for message authentication code calculation during the PACE secure messaging.
	FCS_COP.1/CA_MAC	RP_SFR-SERV	FCS_COP.1.1[AESMAC] or FCS_COP.1.1[DESMAC] is applied for message authentication code calculation during the CA secure messaging.
	FCS_COP.1/SIG_VER	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA.
	FCS_COP.1/EMRTD	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature generation for Active Authentication protocol.
	FIA_UAU.5/PACE	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes. FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during secure

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
			messaging (based on Personalisation Agent Key) to verify the message authentication codes. FCS_COP1.1[SHA] is applied for public key compression (in case DH).
	FIA_UAU.6/PACE	RP_SFR-SERV	FCS_COP1.1[DESMAC] or FCS_COP1.1[AESMAC] is applied during PACE secure messaging the verify the message authentication codes
	FIA_UAU.6/EAC	RP_SFR-SERV	FCS_COP1.1[AESMAC] is applied during CA secure messaging to verify the message authentication codes.
	FIA_API.1	RP_SFR-SERV	FCS_COP.1.1[SHA] and FCS_COP.1.1[ECDH_P1363] are applied to generate the session keys and FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate the message authentication codes.
	FIA_API.1/AA	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature generation for Active Authentication protocol.
	FIA_API.1/PACE-CAM	RP_SFR-SERV	FCS_COP.1.1[SHA] and FCS_COP.1.1[ECDH_P1363] are applied to generate the session keys and FCS_COP.1.1[DESMAC] or FCS_COP.1.1[AESMAC] is applied to generate the message authentication codes
	FDP_UCT.1/TRM	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] is applied during secure messaging to protect the confidentiality of transmitted and received user data.
	FDP_UIT.1/TRM	RP_SFR-SERV	FCS_COP.1[DESMAC] or FCS_COP.1[AESMAC] is applied during secure messaging to protect the integrity of transmitted and received user data.
	FMT_MTD.3	RP_SFR-SERV	FCS_COP.1.1[RSASignaturePKCS1] or FCS_COP.1.1[ECSignature] is applied for digital signature verification for TA.
	FTP_ITC.1/PACE	RP_SFR-SERV	FCS_COP.1[TripleDES] or FCS_COP.1[AES] and FCS_COP.1[DESMAC] or FCS_COP.1[AESMAC] are applied during secure messaging to protect against disclosure and modification
FCS_RNG.1	FCS_RND.1	RP_SFR-SERV	FCS_RNG.1 is applied for nonce generation related to PACE protocol.
	FIA_UAU.4/PACE	RP_SFR-SERV	FCS_RNG.1 is applied as described below: Fresh nonce for PACE protocol; Fresh random for symmetric authentication mechanism. Generate fresh challenge for TA.
FCS_RNG.1[HDT]	-	IP_SFR	-
FDP_ACC.1[EXT-MEM]	-	IP_SFR	-

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
FDP_ACF.1[SD]	-	IP_SFR	
FDP_ACC.1[SD]	-	IP_SFR	-
FDP_ACF.1[FIREWALL]	-	IP_SFR	
FDP_ACC.2[FIREWALL]	-	IP_SFR	-
FDP_ACC.2[ADEL]	-	IP_SFR	-
FDP_ACC.2[SecureBox]	-	IP_SFR	-
FDP_ACC.2[RM]	-	IP_SFR	-
FDP_ACF.1[ADEL]	-	IP_SFR	-
FDP_ACF.1[EXT-MEM]	-	IP_SFR	-
FDP_ACF.1[SecureBox]	-	IP_SFR	-
FDP_ACF.1[RM]	-	IP_SFR	-
FDP_IFC.1[JCVM]	-	IP_SFR	-
FDP_IFC.2[SC]	-	IP_SFR	-
FDP_IFC.2[CFG]	FMT_LIM.1 FMT_LIM.2	RP_SFR-MECH	FDP_IFC.2[CFG] applied to protect the TOE in operational phase.
FDP_IFC.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_IFF.1[JCVM]	-	IP_SFR	-
FDP_IFF.1[SC]	FMT_MTD.1/INI_DIS FMT_MTD.1/INI_ENA	RP_SFR-MECH	FDP_IFF.1[SC] applied to control the writing of initialization and pre-personalization data as required by FMT_MTD.1/INI_DIS and FMT_MTD.1/INI_ENA
FDP_IFF.1[CFG]	-	IP_SFR	-
FDP_IFF.1[MODULAR-DESIGN]	-	IP_SFR	-
FDP_ITC.2[CCM]	-	IP_SFR	-
FDP_RIP.1[OBJECTS]	-	IP_SFR	-
FDP_RIP.1[ABORT]	-	IP_SFR	-
FDP_RIP.1[APDU]	-	IP_SFR	-
FDP_RIP.1[bArray]	-	IP_SFR	-
FDP_RIP.1[GlobalArray_Refined]	-	IP_SFR	-
FDP_RIP.1[KEYS]	FDP_RIP.1		FDP_RIP.1[KEYS] is applied to destroy the secure message session keys and the PACE ephemeral private key.
FDP_RIP.1[TRANSIENT]	-	IP_SFR	-
FDP_RIP.1[ADEL]	-	IP_SFR	-
FDP_RIP.1[ODEL]	-	IP_SFR	-
FDP_ROL.1[FIREWALL]	-	IP_SFR	-
FDP_ROL.1[CCM]	-	IP_SFR	-
FDP_SDI.2[DATA]	FPT_TST.1	RP_SFR-MECH	FDP_SDI.2[DATA] checks the integrity of specific user data.
FDP_SDI.2[SENSITIVE_RESULT]	-	IP_SFR	-
FDP_UIT.1[CCM]	-	IP_SFR	-
FIA_AFL.1[PIN]	-	IP_SFR	-
FIA_ATD.1[AID]	-	IP_SFR	-
FIA_ATD.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_UID.1[SC]	FIA_UID.1/PACE	RP_SFR-MECH	FIA_UID.1[SC] handled the identifier data of the TOE.
FIA_UID.1[CFG]	-	IP_SFR	-
FIA_UID.1[RM]	-	IP_SFR	-
FIA_UID.2[AID]	-	IP_SFR	-
FIA_UID.1[MODULAR-DESIGN]	-	IP_SFR	-
FIA_USB.1[AID]	-	IP_SFR	-
FIA_USB.1[MODULAR-DESIGN]	-	IP_SFR	-

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
FIA_UAU.1[SC]	FIA_UAU.1/PACE	RP_SFR-MECH	FIA_UAU.1[SC] handled the identifier data of the TOE.
FIA_UAU.2[RM]	-	IP_SFR	-
FIA_UAU.4[SC]	-	IP_SFR	-
FMT_MSA.1[JCRE]	-	IP_SFR	-
FMT_MSA.1[JCVM]	-	IP_SFR	-
FMT_MSA.1[ADEL]	-	IP_SFR	-
FMT_MSA.1[SC]	-	IP_SFR	-
FMT_MSA.1[EXT-MEM]	-	IP_SFR	-
FMT_MSA.1[SecureBox]	-	IP_SFR	-
FMT_MSA.1[CFG]	-	IP_SFR	-
FMT_MSA.1[SD]	-	IP_SFR	-
FMT_MSA.1[RM]	-	IP_SFR	-
FMT_MSA.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MSA.2[FIREWALL-JCVM]	-	IP_SFR	-
FMT_MSA.3[FIREWALL]	-	IP_SFR	-
FMT_MSA.3[JCVM]	-	IP_SFR	-
FMT_MSA.3[ADEL]	-	IP_SFR	-
FMT_MSA.3[EXT-MEM]	-	IP_SFR	-
FMT_MSA.3[SecureBox]	-	IP_SFR	-
FMT_MSA.3[CFG]	-	IP_SFR	-
FMT_MSA.3[SD]	-	IP_SFR	-
FMT_MSA.3[SC]	-	IP_SFR	-
FMT_MSA.3[RM]	-	IP_SFR	-
FMT_MSA.3[MODULAR-DESIGN]	-	IP_SFR	-
FMT_MTD.1[JCRE]	-	IP_SFR	-
FMT_MTD.3[JCRE]	-	IP_SFR	-
FMT_SMF.1	-	IP_SFR	-
FMT_SMF.1[ADEL]	-	IP_SFR	-
FMT_SMF.1[EXT-MEM]	-	IP_SFR	-
FMT_SMF.1[SecureBox]	-	IP_SFR	-
FMT_SMF.1[CFG]	-	IP_SFR	-
FMT_SMF.1[SD]	-	IP_SFR	-
FMT_SMF.1[SC]	-	IP_SFR	-
FMT_SMF.1[RM]	-	IP_SFR	-
FMT_SMF.1[MODULAR-DESIGN]	-	IP_SFR	-
FMT_SMR.1	-	IP_SFR	-
FMT_SMR.1[INSTALLER]	-	IP_SFR	-
FMT_SMR.1[ADEL]	-	IP_SFR	-
FMT_SMR.1[CFG]	-	IP_SFR	-
FMT_SMR.1[SD]	-	IP_SFR	-
FMT_SMR.1[MODULAR-DESIGN]	-	IP_SFR	-
FPR_UNO.1	-	IP_SFR	-
FPT_EMSEC.1	FPT_EMS.1	RP_SFR-MECH	FPT_EMS.1matches the FPT_EMSEC.1 of the Platform.
FPT_FLS.1	FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1 of the Platform ensures the secure state of the TOE as required by FPT_FLS.1
FPT_FLS.1[INSTALLER]	-	IP_SFR	-
FPT_FLS.1[ADEL]	-	IP_SFR	-
FPT_FLS.1[ODEL]	-	IP_SFR	-
FPT_FLS.1[CCM]	-	IP_SFR	-
FPT_FLS.1[MODULAR-DESIGN]	-	IP_SFR	-
FPT_TDC.1	-	IP_SFR	-
FPT_RCV.3[INSTALLER]	-	IP_SFR	-
FPT_PHP.3	FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3 matches the FPT_PHP.3 of the Platform.
FTP_ITC.1[SC]	-	IP_SFR	-

Platform-SFR	Corresponding TOE SFR	Category of Platform's SFR	Remarks
ADV_SPM.1	-	IP_SFR	-

5. Table Mapping of Security requirements

101 The FMT_LIM.1 and FMT_LIM.2 are not covered directly by [7]. As described in [17] the purposes of these SFRs is to prevent misuse of test features of the TOE over the life cycle phases

102 According to [7] the Platform consists of the Micro Controller, Crypto Library and Operation System, which are certified as well. By the Micro Controller the limited availability and capability of test features are ensured after Manufacturing phase of the TOE. FMT_LIM.1 and FMT_LIM.2 are covered by the following Security Function of Micro Controller ST: TSF.Control. For details please check [31].

103 To sum up the above-mentioned Security Functions of Micro Controller ensure that the test features of TOE cannot be misused.

104 The Personalization Agent (FMT_SMR.1/PACE) may use the GlobalPlatform function of the Platform.

105 The TOE initialization and pre-personalization (FMT_SMF.1) rely on the Platform functions.

2.5.5 Assurance requirements

106 This ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

107 The Platform-ST [7] requires EAL 6 according to Common Criteria V3.1 R5 augmented by: ASE_TSS.2 and ALC_FLR.1.

108 As EAL 6 covers all assurance requirements of EAL 4 all non-augmented parts of this ST will match to the Platform-ST [7] assurance requirements.

2.6 Analysis

109 Overall there is no conflict between security requirements of this ST and the Platform-ST.

3 Security Problem Definition

110 This ST claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the definition of all Assets, Assumptions, Threats and Organisational Security Policies from the Protection Profiles without repeating these here.

3.1 Assets

111 The Assets included from the Protection Profiles:

- User data stored on the TOE Primary Asset from [18];
- User data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE) Primary Asset from [18];
- Travel document tracing data from Primary Asset [18];
- Accessibility to the TOE functions and data only for authorised subjects Secondary Asset from [18];
- Genuineness of the TOE Secondary Asset from [18];
- TOE internal secret cryptographic keys cryptographic material Secondary Asset from [18];
- TOE internal non-secret cryptographic material from [18];
- Travel document communication establishment authorisation data Secondary Asset from [18];
- Logical travel document sensitive User Data from [17];
- Authenticity of the travel document's chip from [17].

3.2 Subjects

112 Subjects included from the Protection Profiles:

- Travel document holder from [18];
- Travel document presenter (traveller) from [18];
- Terminal from [18];
- Basic Inspection System with PACE (BIS-PACE) from [18];
- Document Signer (DS) from [18];
- Country Signing Certification Authority (CSCA) from [18];
- Personalisation Agent from [18];
- Manufacturer from [18];
- Attacker from [18];
- Country Verifying Certification Authority from [17];
- Document Verifier from [17];
- Terminal from [17];
- Inspection system (IS) from [17];
- Attacker from [17].

3.3 Assumptions

113 The Assumptions included from the Protection Profiles are:

- A.Passive_Auth from [18];
- A.Insp_Sys from [17];
- A.Auth_PKI from [17].

3.4 Threats

114 The Threats included from the Protection Profiles are:

- T.Skimming from [18]
- T.Eavesdropping from [18]
- T.Tracing from [18]
- T.Forgery from [18]
- T.Abuse-Func from [18]
- T.Information_Leakage from [18]
- T.Phys-Tamper from [18]
- T.Malfunction from [18]
- T.Read_Sensitive_Data from [17]
- T.Counterfeit from [17]

3.5 Organisational Security Policies

115 The Organisational Security Policies included from the Protection Profiles are:

- P.Manufact from [18]
- P.Pre-Operational from [18]
- P.Card_PKI from [18]
- P.Trustworthy_PKI from [18]
- P.Terminal from [18]
- P.Sensitive_Data from [17]
- P.Personalisation from [17]

116 **10. Application note (from the ST author)**

Active Authentication Mechanism is an alternative to the Chip Authentication for identifying the TOE. Therefore security problem definition as defined by the protection profiles does not change, as the corresponding elements are already addressed by Chip Authentication.

4 Security Objectives

117 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the definition of all Security Objectives for the TOE and Security Objectives for the Operational Environment from the Protection Profiles without repeating these here.

4.1 Security Objectives for the TOE

118 The Security Objectives for the TOE included from the Protection Profiles are:

- OT.Data_Integrity from [18]
- OT.Data_Authenticity from [18]
- OT.Data_Confidentiality from [18]
- OT.Tracing from [18]
- OT.Prot_Abuse-Func from [18]
- OT.Prot_Inf_Leak from [18]
- OT.Prot_Phys-Tamper from [18]
- OT.Prot_Malfunction from [18]
- OT.Identification from [18]
- OT.AC_Pers from [18]
- OT.Sens_Data_Conf from [17]
- OT.Chip_Auth_Proof from [17]

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

OT.Active_Auth_Proof

Proof of the electronic document's chip authenticity

The TOE shall support the Basic Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Active Authentication as defined in [13]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

The following Security Objective for the TOE is defined in addition to the objectives given by the Protection Profiles to cover the PACE- Chip Authentication mapping mechanism.

OT.Chip_Auth_Proof_PACE_CAM

Proof of the electronic document's chip authenticity

The TOE must support the terminals to verify the identity and authenticity of the Electronic document's chip as issued by the identified issuing State or Organization by means of the PACE-Chip Authentication Mapping (PACE-CAM) as defined in [14]. The authenticity proof provided by electronic document's chip shall be protected against attacks with high attack potential.

120 **11. Application note (from ST author)**

PACE-CAM enables much faster authentication of the of the chip than running PACE with General Mapping (according to [9]) followed by CA1. OT.Chip_Auth_Proof_PACE_CAM is intended to require the Chip to merely provide an additional means – with the same level of security – of authentication.

4.2 Security Objectives for the Operational Environment

121 The Security Objectives for the Operational Environment included from the Protection Profiles are:

- OE.Legislative_Compliance from [18]
- OE.Passive_Auth_Sign from [18]
- OE.Personalisation from [18]
- OE.Terminal from [18]
- OE.Travel_Document_Holder from [18]
- OE.Auth_Key_Travel_Document from [17]
- OE.Authoriz_Sens_Data from [17]
- OE.Exam_Travel_Document from [17]
- OE.Prot_Logical_Travel_Document from [17]
- OE.Ext_Insp_Systems from [17]

122 The following Security Objectives for the Operational Environment are defined in addition to the objectives given by the Protection Profiles to cover the Active Authentication mechanism (OE.Active_Auth_Key_Travel_Document).

123 ***OE.Active_Auth_Key_Travel_Document***

Travel document Active Authentication Key

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Active Authentication Key Pair if necessary, (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 organisations to verify the authenticity of the travel document's chip used for genuine travel document by proof the authenticity of the active authentication public key by Passive Authentication.

124 **12. Application note (from the ST author)**

Active Authentication Mechanism is an alternative to the Chip Authentication for identifying the TOE.

4.3 Security Objective Rationale

125 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the rationale for the definition of all Security Objectives for the TOE and Security Objectives for the Operational Environment from the Protection Profiles without repeating these here.

126 In addition to the rationale given by the Protection Profiles, the threat **T.Counterfeit** "Counterfeit of travel document's chip data" is thwarted through the chip by an identification and authenticity proof required by **OT.Active_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing state or organisation. The Active Authentication public key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** "Travel Document Active Authentication Key".

OT.Chip_Auth_Proof_PACE_CAM ensures that the chip in addition to CA1 also supports the PACE-Chip Authentication Mapping (PACE-CAM) protocol, which supports the same security functionality as CA does. PACE-CAM enables much faster authentication of the of the chip than running PACE with general mapping followed by CA.

127 The following table is copied here from the [17], supplemented by the Threats and Objectives added by the creator of the current Security Target. The items from PP [18] are set in *italic*, and the items added in this ST are set in **bold**.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	**OT.Active_Auth_Proof**	**OE.Auth_Key_Travel_Document**	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance	OE.Active_Auth_Key_Travel_Document
T.Read_Sensitive_Data	x														x			x						
T.Counterfeit		x											X	x		x								X
T.Skimming				x	x	x																x		
T.Eavesdropping						x																		
T.Tracing							x															x		
T.Abuse-Func								x																
T.Information_Leakage									x															
T.Phys-Tamper											x													
T.Malfunction												x												
T.Forgery			x	x	x			x			x					x			x	x	x			
P.Sensitive_Data	x														x			x						
P.Personalisation			x							x									x					
P.Manufact										x														
P.Pre-Operational			x							x									x				x	
P.Terminal																x					x			
P.Card_PKI																				x				
P.Trustworthy_PKI																				x				
A.Insp_Sys																x	x							
A.Auth_PKI															x			x						
A.Passive_Auth																x				x				

6. Table Security Objective Rationale

5 Extended Components Definition

128 This security target claims strict conformance to the Protection Profile [18] given in section 2.2. Therefore this security target includes the definition of all Extended Components from the Protection Profiles without repeating these here.

129 The Extended Components included from the Protection Profiles are:

- FIA_API from [17]
- FAU_SAS from [18]
- FCS_RND from [18]
- FMT_LIM from [18]
- FPT_EMS from [18]

6 Security Requirements

130 The CC allows several operations to be performed on security requirements (on the component level); *refinement, selection, assignment* and *iteration* are defined in sec. 8.1 of Part 1 [1] of the CC. Each of these operations is used in this ST.

131 The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and removed words are crossed out.

132 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*. Selections filled in by the ST author are denoted as double underlined text and a foot note where the selection choices from the PP are listed.

133 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicised like *this*. Assignments filled in by the ST author are denoted as double underlined text.

134 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. For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

135 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the definition of all subjects, objects and operations from the Protection Profiles without repeating these here.

136 The following objects are defined in addition to the objects defined by the Protection Profiles to cover the Active Authentication mechanism:

Name	Data
Active Authentication Key Pair	The Active Authentication Key Pair (KPr_{AA}, $KPuI_{AA}$) is used for the Active Authentication mechanism according to [13].
Active Authentication Public Key (KPu_{AA})	The Active Authentication Public Key (KPu_{AA}) is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical travel document and used by the inspection system for Active Authentication of the travel document's chip. It is part of the user data provided by the TOE for the IT environment. A hash representation of DG15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D).
Active Authentication PrivateKey (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

7. Table Additionally defined objects in this ST

6.1 Security Functional Requirements for the TOE

137 The following sections group the security functional requirements for the TOE is according to the main security functionality.

6.1.1 Class FCS Cryptographic Support

6.1.1.1 Cryptographic key generation (FCS_CKM)

FCS_CKM.1/DH_PACE

Cryptographic key generation – Diffie-Hellman for PACE session keys (taken from [18])

138

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 FCS_CKM.4
FCS_CKM.1.1/DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Diffie- Hellman-Protocol compliant to PKCS#3 and ECDH compliant to [27][28][4,5] and specified cryptographic key sizes ECC 160, 192, 224, 256, 384, 512, 521 bits, RSA 1024, 1280, 1536, 1984, 2048, 4096 bit[6] that meet the following: [14].[7]

139 **13. Application note (from the ST author)**

The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [14]. This protocol is based on the ECDH compliant to TR-03111 [26] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [14] and [26] for details). The shared secret value *K* is used for deriving the AES or 3DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [14] or the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

140 **14. Application note (taken from application note 27 from [18])**

FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [14].

[4] [selection: *Diffie- Hellman-Protocol compliant to PKCS#3, ECDH compliant to [26]*]
[5] [assignment: *cryptographic key generation algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]

FCS_CKM.1/CA

Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys (taken from [17])

141

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 FCS_CKM.4 Cryptographic key destruction: fulfilled FCS_CKM.4
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm based on the key Diffie-Hellman protocol compliant to PKCS#3 and based on an ECDH protocol compliant to [27][28][8,9] and specified cryptographic key sizes Triple DES 112, 168 bits, AES 128, 192, 256 bits[10] that meet the following: based on an ECDH protocol compliant to [26].[11]

142 **15. Application note (taken from application note 12 from [17])**

FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [9].

143 **16. Application note taken from application note 13 from [17])**

The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [9]. This protocol is based on the ECDH compliant to TR-03110 (i.e. an elliptic curve cryptography algorithm) (cf. [26] for details). The shared secret value is used to derive Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function [9]).

144 **17. Application note (redefined by ST author, taken from application note 14 from [17])**

The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol Version 1 may use SHA-1, SHA-224 and SHA-256 (cf. [9] for the details)

FCS_CKM.1/CA_GEN

Cryptographic key generation – Chip Authentication key

145

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled but justified. Justification: The Chip Authentication key pair cannot be used for a generic cryptographic operation but only for Chip Authentication acc. to FIA_API.1.

[8] [selection: *based on the key Diffie-Hellman key derivation protocol compliant to PKCS#3, based on an ECDH protocol compliant to ISO 15946*]
[9] [assignment: *cryptographic key generation algorithm*]
[10] [assignment*: cryptographic key sizes*]
[11] [selection: *based on the Diffie-Hellman key derivation protocol compliant to [25] and [9], based on an ECDH protocol compliant to [26]*

	FCS_CKM.4: Cryptographic key destruction not fulfilled but justified. Justification: The Chip Authentication key pair cannot be deleted or regenerated.
FCS_CKM.1.1/CA_GEN	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECC and RSA[12] and specified cryptographic key sizes ECC 160, 192, 224, 256, 384, 512, 521 bit and RSA 1024, 1280, 1536, 1984, 2048, 4096 bit[13] that meet the following: [14] 4.3.1[14]

146 **18. Application note (from the ST author)**

The Chip Authentication key pair can either be generated in the TOE or imported by the Personalisation Manager (cf. FMT_MTD.1/CAPK). This SFR has been included as required by [17] (see Application Note 44 of [17] after FMT_MTD.1/CAPK). This SFR has been included in this ST in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

FCS_CKM.1/AA_GEN

Cryptographic key generation – Active Authentication key

147	Hierarchical to:	No other components.
	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled but justified. Justification: The Active Authentication key pair cannot be used for a generic cryptographic operation but only for Active Authentication acc. to FIA_API.1/AA. FCS_CKM.4: Cryptographic key destruction: not fulfilled but justified. Justification: The Active Authentication key pair cannot be deleted or regenerated.
	FCS_CKM.1.1/AA_GEN	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECC and RSA[15] and specified cryptographic key sizes ECC 160, 192, 224, 256, 384, 512, 521bits and RSA 1024, 1280, 1536, 1984, 2048, 4096 bit [16] that meet the following: [13].[17]

148 **19. Application note (from the ST author)**

The Active Authentication key pair can either be generated in the TOE or imported by the Personalisation Agent (cf. FMT_MTD.1/AAPK). This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

---

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

FCS_CKM.1/CAM

Cryptographic key generation – PACE-CAM public key and Diffie-Hellman for General Mapping in PACE-GM

149	Hierarchical to:	No other components.
	Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: fulfilled by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
	FCS_CKM.1.1/CAM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PACE-CAM in combination with PACE-GM[18] and specified cryptographic key sizes AES 128, 192 and 256 bit[19] that meet the following: [13][20]

FCS_CKM.4

Cryptographic key destruction – Session keys (taken from [18])

150	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 physically overwriting the keys in a randomized manner[21] that meets the following: none.[22]

151 **20. Application note (from the ST author)**

The TOE destroys any session keys after detection of an error in verification of the MAC of a received command. The PACE Session Keys are destroyed after generation of the Chip Authentication Session Key (i.e. successfully performing the Chip Authentication) and changing the secure messaging to the Chip Authentication Session Keys. The TOE clears the memory area of any session keys in secure way 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.

6.1.1.2 Cryptographic operation (FCS_COP)

FCS_COP.1/PACE_ENC

Cryptographic operation – Encryption / Decryption AES / Triple DES (taken from [18])

[18] [assignment: *cryptographic key generation algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]
[21] [assignment: *cryptographic key destruction method*]
[22] [assignment: *list of standards*]

152	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
	FCS_COP.1.1/PACE_ENC	The TSF shall perform secure messaging – encryption and decryption[23] in accordance with a specified cryptographic algorithm AES in CBC or EBC mode or Triple DES[24] in CBC or EBC mode[25] and cryptographic key sizes AES: 128, 192 or 256 bits[26]; Triple DES: 112 or 168 bit[27] that meet the following: compliant to [27][14].[28]

21. Application note (taken from application note 29 from [18])

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

FCS_COP.1/PACE_MAC

Cryptographic operation – MAC (taken from [18])

154	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 secure messaging – message authentication code[29] in accordance with a specified cryptographic algorithm CMAC or Retail-MAC[30,31] and cryptographic key sizes Triple DES: 112, 168 or AES-CMAC: 128, 192 or 256[32] bit[33] that meet the following: compliant to [14].[34]

[23] [assignment: *list of cryptographic operations*]
[24] [selection: *AES, Triple DES*]
[25] [assignment: *cryptographic algorithm*]
[26] [selection: *112, 128, 192, 256*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of standards*]
[29] [assignment: *list of cryptographic operations*]
[30] [selection: *CMAC, Retail-MAC*]
[31] [assignment: *cryptographic algorithm*]
[32] [selection: *112, 128, 192, 256*]
[33] [assignment: *cryptographic key sizes*]
[34] [assignment: *list of standards*]

155 **22. Application note (from the ST author)**

The TOE implements the cryptographic primitives (i.e. CMAC and Retail-MAC) 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 the PACE protocol according to FCS_CKM.1/DH_PACE.

FCS_COP.1/CA_ENC

Cryptographic operation – Symmetric Encryption / Decryption (taken from [17])

156

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/CA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_CKM.1.1/CA_ENC	The TSF shall perform secure messaging – encryption and decryption[35] in accordance with a specified cryptographic algorithm AES and Triple DES[36] and cryptographic key sizes AES: 128, 192, 256 bits and Triple DES: 112, 168 bits[37] that meet the following: [27] and ICAO TR-SAC [14], chapter 4.3[38]

157 **23. Application note (taken from application note 16 from [17])**

The TOE implements the cryptographic primitives (e.g. Triple DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the symmetric authentication mechanism.

FCS_COP.1/CA_MAC

Cryptographic operation – MAC (taken from [17])

158

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/CA, FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

[35] [assignment: *list of cryptographic operations*]
[36] [assignment: *cryptographic algorithm*]
[37] [assignment: *cryptographic key sizes*]
[38] [assignment: *list of standards*]

FCS_COP.1.1/CA_MAC	The TSF shall perform secure messaging – message authentication code[39] in accordance with a specified cryptographic algorithm CMAC or Retail-MAC[40] and cryptographic key sizes Triple DES: 112, 168 or AES-CMAC: 128, 192 or 256 bit[41] that meet the following: [27] and ICAO TR-SAC [14].[42]

159 **24. Application note (taken from application note 18 from [17]):**

The TOE implements the cryptographic primitives (i.e. CMAC and Retail-MAC) for secure messaging with message authentication code over transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the symmetric authentication mechanism.

FCS_COP.1/SIG_VER

Cryptographic operation – Signature verification by travel document (taken from [17])

160

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/CA FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
FCS_COP.1.1/SIG_VER	The TSF shall perform digital signature verification[43] in accordance with a specified cryptographic algorithm RSA PKCS#1 v2.2, RSA PKCS#1-PSS and ECDSA with SHA-1, SHA-224, SHA-256 SHA-384 and SHA-512[44] and cryptographic key sizes ECC 160, 192, 224, 256, 320, 384, 521 bits RSA 2048 and 4096[45] that meet the following: [27][28]

161 **25. Application note(from the ST author)**

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 when executing Terminal Authentication Version 1.

FCS_COP.1/EMRTD

Cryptographic operation – Signature generation

[39] [assignment: *list of cryptographic operations*]
[40] [assignment: *cryptographic algorithm*]
[41] [assignment: *cryptographic key sizes*]
[42] [assignment: *list of standards*]
[43] [assignment: *list of cryptographic operations*]
[44] [assignment: *cryptographic algorithm*]
[45] [assignment: *cryptographic key sizes*]

162	Hierarchical to:	No other components.
	Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of in user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: This SFR is not used to calculate any shared secrets, nor does it import user data. Therefore there is no need for security attributes. FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.
	FCS_COP.1.1/EMRTD	The TSF shall perform digital signature generation[46] in accordance with a specified cryptographic algorithm RSA PKCS#1 v1.5 and RSA PKCS#1-PSS and ECDSA with SHA-1 SHA-224 SHA-256, SHA-384, SHA-512[47] and cryptographic key sizes RSA 2048-4096 bits, ECC 160, 192, 224, 256, 320, 384, 521,[48] that meet the following [27][28].[49,50]

163 **26. Application note (from the ST author)**

The TOE performs digital signature generation with RSA. This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

FCS_COP.1/CAM

Cryptographic operation – Signature generation

164	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/CAM FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4
	FCS_COP.1.1/CAM	The TSF shall perform the PACE-CAM protocol[51] in accordance with a specified cryptographic algorithm PACE-CAM [52]and cryptographic key sizes AES 128, 192 and 256 bits,[53] that meet the following [10][54,55]

[46] [assignment: *list of cryptographic operations*]
[47] [assignment: *cryptographic algorithm*]
[48] [assignment: *cryptographic key sizes*]
[49] According to [13], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.
[50] [assignment: *list of standards*]
[51] [assignment: *list of cryptographic operations*]
[52] [assignment: *cryptographic algorithm*]
[53] [assignment: *cryptographic key sizes*]
[54] According to [13], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.
[55] [assignment: *list of standards*]

165 **27. Application note (from the ST author)**

Whereas FCS_CKM.1/CAM addresses the Diffie-Hellman based key-derivation, this SFR is concerned with the correct implementation and execution of the whole PACE-CAM protocol. Note that in particular the last protocol step to authenticate the chip towards the terminal is an essential part of the protocol, and not addressed in FCS_CKM.1/CAM.

6.1.1.3 Random Number Generation (FCS_RND.1)

166 The TOE meets the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below [2].

FCS_RND.1

Quality metric for random numbers (taken from [18])

167

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that DRG.3 (high) according to AIS20 [20].[56]

168 **28. Application note (from the ST author)**

The TOE generates random numbers used for the authentication protocols e. g. as required by FIA_UAU.4/PACE.

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

6.1.2 Class FIA Identification and Authentication

169 **29. Application note** (taken from application note 19 from **[17]**)

The 8. Table Overview on authentication SFRs provides an overview of the authentication mechanisms used

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalisation Agents	FIA_UAU.4/PACE
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol	FIA_UAU.5/PACE
PACE protocol	FIA_AFL.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE
Passive Authentication	FIA_UAU.5/PACE
Active Authentication Mechanism	FIA_API.1/AA

8. Table Overview on authentication SFRs

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

- the asymmetric key agreement to establish symmetric secure messaging keys 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.

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

6.1.2.1 Authentication failures (FIA_AFL)

FIA_AFL.1/PACE

Authentication failure handling – PACE authentication using non-blocking authorisation data (taken from [18])

172

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE
FIA_AFL.1.1/PACE	The TSF shall detect when an administrator configurable positive integer within [1-127][57,58] unsuccessful

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

authentication attempt occurs related to authentication attempts using the PACE password as shared password.[59]

173	FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met[60], the TSF shell delay each following authentication attempt until the next successful authentication.[61]

FIA_UID.1/PACE

Timing of identification (taken from [17])

174	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_UID.1.1/PACE	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE Protocol according to [14], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4. to carry out the Chip Authentication Protocol Version 1 according to [9] or the Chip Authentication mapping (PACE-CAM) according to [14], 5. to carry out the Terminal Authentication Protocol Version 1 according to [9] resp. according to [14] if PACE-CAM is used. 6. to carry out the Active Authentication Mechanism[62] on behalf of the user to be performed before the user is identified.
175	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.

176 **30. Application note (taken from application note 21 from [17])**

In the Phase 2 “Manufacturing of the TOE” the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 “Personalisation of the travel document”. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal

[59] [assignment: *list of authentication events*]
[60] [selection: *met ,surpassed*]
[61] [assignment: *list of actions*]
[62] [assignment: *list of TSF-mediated actions*]

Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

177 **31. Application note (taken from application note 22 from [17])**

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

178 **32. Application note (taken from application note 21 from [17])**

In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC. Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

179 **33. Application note (ST author)**

The SFR is refined here in order for the TSF to additionally provide the PACE-CAM protocol by referencing [14]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

Furthermore this SFR is extended because the Active Authentication protocol.

FIA_UAU.1/PACE

Timing of authentication (taken from [17])

180

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE.
FIA_UAU.1.1/PACE	The TSF shall allow 1.to establish the communication channel, 2.carrying out the PACE Protocol according to [14], 3.to read the Initialisation Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS, 4.to identify themselves by selection of the authentication key, 5.to carry out the Chip Authentication Protocol Version 1 according to [9], 6.to carry out the Terminal Authentication Protocol Version 1 according to [9], 7.to carry out the Active Authentication Mechanism[63] on behalf of the user to be performed before the user is authenticated.
FCS_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.

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

181 **34. Application note (taken from application note 25 from [17])**

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 travel document holder itself or an authorised other person or device (Basic Inspection System with PACE). If PACE was successfully performed, secure messaging is started using the derived PACE Session Keys, cf. FTP_ITC.1/PACE.

FIA_UAU.4/PACE

Single-use authentication of the Terminals by the TOE (taken from [17])

182	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1.PACE Protocol according to [14], 2.Authentication Mechanism based on AES or Triple DES,[64,65] 3.Terminal Authentication Protocol Version 1 according to [9]. **4. Active Authentication according to [13].**

183 **35. Application note (from the ST author)**

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.

The Authentication Mechanism mentioned here is the Symmetric Authentication Mechanism also mentioned at the next (FIA_UAU.5/PACE Multiple authentication mechanisms) requirement. This mechanism equals the BAC algorithm with the difference, that the BAC algorithm bases its computations at the data from MRZ, but during the personalization there is no MRZ yet, so as another base, the Chip Serial number was used. Thus the ST and other documents will also refer to this algorithm as the *Basic Access Control Based on Chip Serial Number.*

The refinement was necessary because the authentication data (nonce) is must not be reused during Active Authentication protocol according to [13].

FIA_UAU.5/PACE

Multiple authentication mechanisms (taken from [17])

184	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_UAU.5.1/PACE	The TSF shall provide 1.PACE Protocol according to [13] **and PACE-CAM protocol according to [14]** 2.Passive Authentication according to [13], 3.Secure messaging in MAC-ENC mode according to [14],

[64] [selection: *Triple DES, AES or other approved algorithms*]
[65] [assignment: *identified authentication mechanism(s)*]

4. Symmetric Authentication Mechanism based on Triple DES or AES,[66]

5. Terminal Authentication Protocol Version 1 according to [9],[67]

to support user authentication.

185 FIA_UAU.5.2/PACE — The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.

2. The TOE accepts the authentication attempt as Personalisation Agent by *the Authentication Mechanism with Personalisation Agent Keys*.[68]

3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism Version 1.

4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol Version 1 only if the terminal uses the public key presented during the Chip Authentication Protocol Version 1 and the secure messaging established by the Chip Authentication Protocol Version 1 **or if the terminal uses the public key presented during PACE-CAM and the secure messaging established during PACE.**[69]

5. none[70]

186 **36. Application note (taken from application note 36 from [18])**

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 *eMRTD* application.

187 **37. Application note (from the ST author)**

The second part of this requirement states that if there is already successful PACE, the commands can only be accepted using PACE protocol, if there is already successful Chip Authentication, TOE accepts secure messaging based on the keys of Chip Authentication, or if there is already successful Terminal Authentication, the messaging is based on the Chip Authentication Public Key, but it does not state, that these protocols can follow each other in successive order even in the same session, which is the practice concerning these protocols.

The SFR is refined here in order for the TSF to additionally provide the PACE-CAM protocol by referencing [14]. PACE-CAM combines PACE and Chip Authentication 1 for faster execution times. Hence, a TOE meeting the original requirement also meets the refined requirement.

---

[66] [selection: *Triple DES, AES or other approved algorithms*]
[67] [assignment: *list of multiple authentication mechanisms*]
[68] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]
[69] [assignment: *list of conditions under which re-authentication is required*]
[70] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

FIA_UAU.6/PACE

Re-authenticating of Terminal by the TOE (taken from [18])

188

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/PACE	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[71]

189 **38. Application note (taken from application note 37 from [18])**

The PACE protocol specified in [14] 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

Re-authenticating of Terminal by the TOE (taken from [17])

190

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/EAC	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.[72]

191 **39. Application note (taken from application note 29 from [17])**

The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [13] 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.

FIA_API.1

Authentication Proof of Identity (taken from [17])

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

192	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_API.1.1	The TSF shall provide a Chip Authentication Protocol Version 1 according to [9][73] to prove the identity of the TOE.[74]

193 **40. Application note (taken from application note 30 from [17])**

The TOE implements the Chip Authentication Mechanism v1 specified in [9]. 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 [13]. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA

Authentication Proof of Identity – travel document

194	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_API.1.1/AA	The TSF shall provide the Active Authentication Mechanism according to [13][75] to prove the identity of the TOE.[76]

195 **41. Application note (from the ST author)**

The SFR FIA_API.1/AA has been included in this ST in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

196 The following SFR is newly defined in this ST and addresses the PACE-CAM protocol.

FIA_API.1/PACE-CAM

Authentication Proof of Identity

197	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FIA_API.1.1/PACE_CAM	The TSF shall provide the protocol PACE-CAM [14][77], to prove the identity of the TOE[78].

[73] [assignment: *authentication mechanism*]
[74] [assignment: *authorized user or role*]
[75] [assignment: *authentication mechanism*]
[76] [assignment: *authorized user or role*]

6.1.3 Class FDP User Data Protection

6.1.3.1 Access control policy (FDP_ACC)

FDP_ACC.1/TRM

Subset access control (taken from [17])

198	Hierarchical to:	No other components.
	Dependencies:	FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM
	FDP_ACC.1.1/TRM	The TSF shall enforce the Access Control SFP[79] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document.[80]

6.1.3.2 Access control functions (FDP_ACF)

FDP_ACF.1/TRM

Security attribute based access control (taken from [17])

199	Hierarchical to:	No other components
	Dependencies:	FDP_ACC.1 Subset access control: fulfilled by FDP_ACC.1/TRM FMT_MSA.3 Static attribute initialisation: not fulfilled, but justified: The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalisation 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.
200	FDP_ACF.1.1/TRM	The TSF shall enforce the Access Control SFP[81] to objects based on the following: 1. Subjects: a. Terminal, b. BIS-PACE; c. Extended Inspection System. 2. Objects: a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 , EF.SOD and EF.COM of the logical travel document, b. data in EF.DG3 of the logical travel document , c. data in EF.DG4 of the logical travel document , d. all TOE intrinsic secret cryptographic keys stored in the travel document.[82] 3. Security attributes:

[79] [assignment: *access control SFP*]
[80] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[81] [assignment: *access control SFP*]
[82] [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]

a. PACE Authentication,

b. Terminal Authentication Version 1,

c. Authorisation of the Terminal.[83]

201 FDP_ACF.1.2/TRM

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

A BIS-PACE is allowed to read data objects from FDP_ACF.1/TRM according to [14] after a successful PACE authentication as required by FIA_UAU.1/PACE.[84]

202 FDP_ACF.1.3/TRM

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[85]

203 FDP_ACF.1.4/TRM

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.

2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.

3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.

5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.

6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.[86]

204 **42. Application note (taken from application note 33 from [17])**

The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [9]. 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.

---

[83] [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*]

[84] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

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

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

205 **43. Application note (taken from application note 34 from [17])**

Please note that the Document Security Object (SO_D) stored in EF.SOD (see [13]) does not belong to the user data, but to the TSF-data. The Document Security Object can be read out by the PACE authenticated BIS-PACE, see [13].

206 **44. Application note (taken from application note 41 from [18])**

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

207 **45. Application note (taken from application note 35 from [17])**

FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The PACE and the Chip Authentication Protocol Version 1 establish different session keys to be used for secure messaging.

6.1.3.3 Residual information protection (FDP_RIP)

FDP_RIP.1

Subset residual information protection (taken from [18])

208	Dependencies:	No dependencies.
	FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[87] the following objects: 1. Session Keys (immediately after closing related communication session), 2. the ephemeral private key ephem-SK_{PICC}-PACE (by having generated a DH shared secret *K* [88]),[89] 3. none.[90]

209 46. Application note (taken from application note 42 from [18])

The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1 requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard.

6.1.3.4 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

FDP_UCT.1/TRM

Basic data exchange confidentiality – MRTD (taken from [18])

210	Hierarchical to:	No other components.

[87] [selection: *allocation of the resource to, deallocation of the resource from*]
[88] according to [14]
[89] [assignment: *list of objects*]
[90] [assignment: *list of objects*].

	Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
	FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP[91] to be able to transmit and receive[92] user data in a manner protected from unauthorised disclosure.

6.1.3.5 Inter-TSF user data integrity transfer protection (FDP_UCT)

FDP_UIT.1/TRM

Data exchange integrity (taken from [18])

211	Hierarchical to:	No other components.
	Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] fulfilled by FTP_ITC.1/PACE [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/TRM
	FDP_UIT.1.1/TRM	The TSF shall enforce the Access Control SFP[93] to be able to transmit and receive[94] user data in a manner protected from modification, deletion, insertion and replay[95] errors.
	FDP_UIT.1.2/TRM	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[96] has occurred.

6.1.4 Class FAU Security Audit

6.1.4.1 Audit Storage (FAU_SAS)

FAU_SAS.1

Audit storage (taken from [18])

212	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FAU_SAS.1.1	The TSF shall provide the Manufacturer[97] with the capability to store the Initialisation and Pre-Personalisation Data[98] in the audit records.

[91] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[92] [selection: *transmit, receive*]
[93] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[94] [selection: *transmit, receive*]
[95] [selection: *modification, deletion, insertion, replay*]
[96] [selection: *modification, deletion, insertion, replay*]
[97] [assignment: *list of audit information*]
[98] [assignment: *list of management functions to be provided by the TSF*]

213 **47. Application note (taken from application note 46 from [18])**

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

6.1.5 Class FMT Security Management

214 The SFR FMT_SMF.1 and FMT_SMR.1/PACE provide basic requirements on the management of the TSF data.

6.1.5.1 Specification of Management Functions (FMT_SMF)

FMT_SMF.1

Specification of Management Functions (taken from [18][17])

215

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Initialization , 2. Pre-personalisation , 3. Personalisation 4. Configuration.[99]

6.1.5.2 Security management roles (FMT_SMR)

FMT_SMR.1/PACE

Security roles (taken from [17])

216

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE
FMT_SMR.1.1/PACE	The TSF shall maintain the roles 1. Manufacturer, 2. Personalisation Agent, 3. Terminal, 4. PACE authenticated BIS-PACE, 5. Country Verifying Certification Authority, 6. Document Verifier, 7. Domestic Extended Inspection System, 8. Foreign Extended Inspection System.[100]

[99] [assignment: *list of management functions to be provided by the TSF*]
[100] [assignment: *the authorised identified roles*]

217	FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.

6.1.5.3 Limited capabilities (FMT_LIM)

FMT_LIM.1

Limited capabilities (taken from [17])

218	Hierarchical to:	No other components.
	Dependencies:	FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2
	FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.[101]

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

FMT_LIM.2

Limited availability (taken from [17])

219	Hierarchical to:	No other components.
	Dependencies:	FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.1
	FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying test features after TOE delivery do not allow 1. User Data to be manipulated and disclosed, 2. TSF data to be manipulated or disclosed, 3. software to be reconstructed, 4. substantial information about construction of TSF to be gathered which may enable other attacks and 5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.[102]

220 **48. Application note (taken from application note 39 from [17])**

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

[101] [assignment: *Limited capability and availability policy*]
[102] [assignment: *Limited capability and availability policy*]

respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

221 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.

6.1.5.4 Management of TSF data (FMT_MTD)

FMT_MTD.1/CVCA_INI

Management of TSF data – Initialisation of CVCA Certificate and Current Date (taken from [17])

222

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/CVCA_INI	The TSF shall restrict the ability to write[103] the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date[104] 4. none[105] to the Personalisation Agent[106]

223 **49. Application note (from the ST author)**

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 Authorisation.

FMT_MTD.1/CVCA_UPD

Management of TSF data – Country Verifying Certification Authority (taken from [17])

224

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/CVCA_UPD	The TSF shall restrict the ability to update[107] the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate[108] to Country Verifying Certification Authority.[109]

[103] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[104] [assignment: *list of TSF data*]
[105] [assignment: *list of TSF data*]
[106] [assignment: *the authorised identified roles*]
[107] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[108] [assignment: *list of TSF data*]
[109] [assignment: *the authorised identified roles*]

225 **50. Application note (taken from application note 42 from [17])**

The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [9]). 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. [9]).

FMT_MTD.1/DATE

Management of TSF data – Current date (taken from [17])

226

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/DATE	The TSF shall restrict the ability to modify[110] the Current date[111] to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System[112].

227 **51. Application note (taken from application note 43 from [17])**

The authorized roles are identified in their certificate (cf. [9]) 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 v.1 (cf. to [9]).

FMT_MTD.1/CAPK

Management of TSF data – Chip Authentication Private Key (taken from [17])

228

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/CAPK	The TSF shall restrict the ability to create, load[113] the Chip Authentication Private Key[114] to the Manufacturer and the Personalisation Agent.[115]

229 **52. Application note (from the ST author)**

The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself. This key generation is covered by FCS_CKM.1/CA_GEN.

---

[110] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[111] [assignment: *list of TSF data*]
[112] [assignment: *the authorised identified roles*]
[113] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[114] [assignment: *list of TSF data*]
[115] [assignment: *the authorised identified roles*]

FMT_MTD.1/INI_ENA

Management of TSF data – Writing Initialisation and Pre-personalisation Data (taken from [18])

230	Hierarchical to:	No other components.
	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
	FMT_MTD.1.1/INI_ENA	The TSF shall restrict the ability to write[116] the Initialisation Data and Pre-personalisation Data[117] to the Manufacturer.[118]

FMT_MTD.1/INI_DIS

Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data (taken from [18])

231	Hierarchical to:	No other components.
	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
	FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to read out[119] the Initialisation Data and the Pre-personalisation Data[120] to the Personalisation Agent.[121]

232 **53. Application note (taken from application note 49 from [18])**

The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

FMT_MTD.1/KEY_READ

Management of TSF data – Key Read (taken from [17])

233	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

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

FMT_MTD.1.1/KEY_READ	The TSF shall restrict the ability to read[122] the 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalisation Agent Keys, 4. **Active Authentication Private Key**[123] to none.[124]

234 **54. Application note (from the ST author)**

A refinement has been added to this SFR to also cover the private key for the Active Authentication mechanism.

FMT_MTD.1/PA

Management of TSF data – Personalisation Agent (taken from [18])

235	Hierarchical to:	No other components.
	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
	FMT_MTD.1.1/PA	The TSF shall restrict the ability to write[125] the Document Security Object (SO_D)[126] to the Personalisation Agent.[127]

236 **55. Application note (taken from application note 50 from [18])**

By writing SOD into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

FMT_MTD.1/AAPK

Management of TSF data – Active Authentication Private Key

237	Hierarchical to:	No other components.
	Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE
	FMT_MTD.1.1/AAPK	The TSF shall restrict the ability to create, load[128] the Active Authentication Private Key[129] to the Personalisation Agent.[130]

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

238 **56. Application note (from the ST author)**

This SFR has been included in this security target in addition to the SFRs defined by the Protection Profiles claimed in clause 2.2. This extension does not conflict with the strict conformance to the claimed Protection Profiles.

FMT_MTD.3

Secure TSF data (taken from [17])

239

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data: fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol Version 1 and the Access Control.[131]

240 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 Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the 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.

241 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.

242 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.

243 **57. Application note (taken from application note 46 from [17])**

The Terminal Authentication Version 1 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.

6.1.6 Class FPT Protection of the Security Functions

244 The TOE shall prevent inherent and forced illicit information leakage for the 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 design measures to be described within the SAR 'Security architecture description' (ADV_ARC.1) prevent bypassing,

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

deactivation and manipulation of the security features or misuse of the TOE security functionality.

6.1.6.1 TOE Emanation (FPT_EMS)

FPT_EMS.1

TOE Emanation (taken from [17])

245

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit variations in power consumption or timing during command execution [132] in excess of non useful information[133] enabling access to 1. Chip Authentication Session Keys 2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. the ephemeral private key $SK_{MapPICC}$-PACE-CAM[134] 5. Personalisation Agent Key(s) and 6. Chip Authentication Private Key and 7. Active Authentication Private Key [135]
246 FPT_EMS.1.2	The TSF shall ensure any users[136] are unable to use the following interface smart card circuit contacts[137] to gain access to 1. Chip Authentication Session Key(s) 2. PACE session keys (PACE-K_{MAC}, PACE-K_{Enc}), 3. the ephemeral private key ephem-SK_{PICC}-PACE, 4. the ephemeral private key $SK_{MapPICC}$-PACE-CAM[138] 5. Personalisation Agent Key(s) 6. Chip Authentication Private Key(s) 7. Active Authentication Private Key[139]

247 **58. Application note (taken from application note 51 from [18])**

The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip has to provide a smart card contactless interface, but may have also (not used by the terminal, but maybe by an attacker) sensitive contacts according to ISO/IEC 7816-2 as well. Examples of measurable phenomena include,

---

[132] [assignment: *types of emissions*]
[133] [assignment: *specified limits*]
[134] [assignment: *list of types of TSF data*],
[135] [assignment: *list of type of users data*]
[136] [assignment: *type of users*]
[137] [assignment: *type of connection*]
[138] [assignment: *list of types of TSF data*],
[139] [assignment: *list of types of TSF data*]

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.

248 **59. Application note (from ST author)**

W.r.t. PACE-CAM, note the significance of protecting $SK_{Map,PICC}$-PACE-CAM: Whereas when running PACE and CA separately, gaining knowledge of the ephemeral key SK_{PICC}-PACE enables the attacker to decrypt the current PACE session, an attacker that gains knowledge of the ephemeral key $SK_{Map,PICC}$-PACE-CAM can not only decrypt the session but also easily reveal the static secret chip authentication key SK_{PICC}: Let ° denote the group operation (i.e. addition or multiplication), and let i(x) denote the inverse of x. Since the chip sends CA_{PICC} = $SK_{Map,PICC}$-PACE-CAM ° i(SK_{PICC}) to the terminal, a malicious attacker that gains knowledge of $SK_{Map,PICC}$-PACE-CAM can reveal SK_{PICC} by computing SK PICC = i(CA_{PICC}) ° $SK_{Map,PICC}$-PACE-CAM.

Because of the Active Authentication is supported protocol by the TOE, the SFR is extended with Active Authentication Private Key.

6.1.6.2 Fail secure (FPT_FLS)

FPT_FLS.1

Failure with preservation of secure state (taken from [18])

249	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. none[140]

6.1.6.3 TSF self test (FPT_TST)

FPT_TST.1

TSF testing (taken from [18])

250	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FPT_TST.1.1	The TSF shall run a suite of self tests during initial start-up, periodically during normal operation,[141][142] to demonstrate the correct operation of the TSF.[143]
	FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.[144]

[140] [assignment: *list of types of failures in the TSF*]
[141] [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*]
[142] [assignment: *conditions under which self test should occur*]
[143] [selection: *[assignment: parts of TSF], the TSF*]
[144] [selection: *[assignment: parts of TSF], TSF data*]

	FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.[145]

6.1.6.4 TSF physical protection (FPT_PHP)

FPT_PHP.3

Resistance to physical attack (taken from [18])

251

	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[146] to the TSF[147] by responding automatically such that the SFRs are always enforced.

252 **60. Application note (taken from application note 53 from [18])**

The TOE implements 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.

6.1.7 Class FTP Trusted Path/Channels

6.1.7.1 Inter-TSF trusted channel (FTP_ITC)

FTP_ITC.1/PACE

Inter-TSF trusted channel after PACE

253

	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
	FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
	FTP_ITC.1.3/PACE	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.[148]

254 **61. Application note (taken from application note 43 from [18])**

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.

---

[145] [selection: *[assignment: parts of TSF], TSF*]
[146] [assignment: *physical tampering scenarios*]
[147] [assignment: *list of TSF devices/elements*]
[148] [selection: *modification, deletion, insertion, replay*]

255 **62. Application note (taken from application note 44 from [18])**

The trusted channel is established after successful performing 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}): 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 PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

256 **63. Application note (taken from application note 45 from [18])**

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

6.2 Security Assurance Requirements for the TOE

257 The assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

64. Application note (taken from application note 49 from [17])

The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (OE.Prot_Logical_Travel_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

258 The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.

	OT.Sens_Data_Conf	*OT.Chip_Auth_Proof*	*OT.AC_Pers*	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Identification*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Tracing*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*	*OT.Active_Auth_Proof*	*OT.Chip_Auth_Proof_PACE_CAM*
FCS_CKM.1/DH_PACE	-	-	-	X	X	X	-	-	-	-	-	-	-	-

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof	OT.Chip_Auth_Proof_PACE_CAM
FCS_CKM.1/CA	X	X	X	X	X	X	-	-	-	-	-	-	-	-
FCS_CKM.1/CA_GEN	X	X	X	X	X	X	-	-	-	-	-	-	-	-
FCS_CKM.1/AA_GEN	-	-	-	-	-	-	-	-	-	-	-	-	X	-
FCS_CKM.1/CAM	-	-	-	X	X	X	-	-	-	-	-	-	-	X
FCS_CKM.4	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FCS_COP.1/PACE_ENC	-	-	-	-	-	X	-	-	-	-	-	-	-	-
FCS_COP.1/PACE_MAC	-	-	-	X	X		-	-	-	-	-	-	-	-
FCS_COP.1/CA_ENC	X	X	X	X		X	-	-	-	-	-	-	-	-
FCS_COP.1/CA_MAC	X	X	X	X	-	-	-	-	-	-	-	-	-	-
FCS_COP.1/SIG_VER	X	-	X	-	-	-	-	-	-	-	-	-	-	-
FCS_COP.1/EMRTD	-	-	-	-	-	-	-	-	-	-	-	-	X	-
FCS_COP.1/CAM	-	-	-	X	X	X	-	-	-	-	-	-	-	X
FCS_RND.1	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_AFL.1/PACE	-	-	-	-	-	-	-	-	-	X	-	-	-	-
FIA_UID.1/PACE	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.1/PACE	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.4/PACE	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.5/PACE	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.6/PACE	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FIA_UAU.6/EAC	X	-	X	X	X	X	-	-	-	-	-	-	-	-
FIA_API.1	-	X	-	-	-	-	-	-	-	-	-	-	-	-
FIA_API.1/AA	-	-	-	-	-	-	-	-	-	-	-	-	X	-
FIA_API.1/PACE-CAM	-	-	-	X	X	X	-	-	-	-	-	-	-	X
FDP_ACC.1/TRM	X	-	X	X	-	X	-	-	-	-	-	-	-	-
FDP_ACF.1/TRM	X	-	X	X	-	X	-	-	-	-	-	-	-	-
FDP_RIP.1	-	-	-	X	X	X	-	-	-	-	-	-	-	-
FDP_UCT.1/TRM	X	-	-	X	-	X	-	-	-	-	-	-	-	-
FDP_UIT.1/TRM	-	-	-	X	-	X	-	-	-	-	-	-	-	-
FAU_SAS.1	-	-	X	-	-	-	X	-	-	-	-	-	-	-
FMT_SMF.1	-	X	X	X	X	X	X	-	-	-	-	-	-	-
FMT_SMR.1/PACE	-	X	X	X	X	X	X	-	-	-	-	-	-	-

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof	OT.Chip_Auth_Proof_PACE_CAM
FMT_LIM.1	-	-	-	-	-	-	-	X	-	-	-	-	-	-
FMT_LIM.2	-	-	-	-	-	-	-	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/INI_ENA	-	-	X	-	-	-	X	-	-	-	-	-	-	-
FMT_MTD.1/INI_DIS	-	-	X	-	-	-	X	-	-	-	-	-	-	-
FMT_MTD.1/KEY_READ	X	X	X	X	X	X		-	-	-	-	-	-	-
FMT_MTD.1/PA	-	-	X	X	X	X		-	-	-	-	-	-	-
FMT_MTD.1/AAPK	-	-	-	-	-	-	-	-	-	-	-	-	X	-
FMT_MTD.3	X	-	-	-	-	-	-	-	-	-	-	-	-	-
FPT_EMS.1	-	-	X	-	-	-	-	-	X	-	-		-	-
FPT_FLS.1	-	-	-	-	-	-	-	-	X	-	-	X	-	-
FPT_TST.1	-	-	-	-	-	-	-	-	X	-	-	X	-	-
FPT_PHP.3	-	-	-	X	-	-	-	-	X	-	X	-	-	-
FTP_ITC.1/PACE	-	-	-	X	X	X	-	-	-	X	-	-	-	-

9 Table Coverage of Security Objective for the TOE by SFR

259 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the Security Requirements Rationale of the Protection Profiles without repeating these here with exception of OT.Chip_Auth_Proof.

260 The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 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. This key can either be written to the TOE as defined by FMT_MTD.1/CAPK or created on the TOE itself as supported by FCS_CKM.1/CA_GEN. The Chip Authentication Protocol v.1 [9] 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).

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

262 The security objective OT.Active_Auth_Proof

"Proof of travel document's chip authenticity" is ensured by the Active Authentication Mechanism [13] 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 can either be written to the TOE as defined by FMT_MTD.1/AAPK or created on the TOE itself as supported by FCS_CKM.1/AA_GEN. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/EMRTD.

263 The **OT.Chip_Auth_Proof_PACE_CAM** is a newly introduced security objective that aims to ensure the authenticity of the electronic document's chip by the PACE-CAM protocol, in particular in the context of an ePassport application. This is supported by FCS_CKM.1/CAM for cryptographic key-generation, and FIA_API.1/PACE-CAM and FCS_COP.1/CAM for the implementation itself, as well as FIA_UID.1/PACE and FIA_UAU.5/PACE, the latter supporting the PACE protocol.

6.3.2 Dependency Rationale

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

265 The dependency analysis has directly been made within the description of each SFR in sec. 6.1 above. All dependencies being expected by CC part 2 and by extended components definition in clause 5 are either fulfilled or their non-fulfilment is justified.

6.3.3 Security Assurance Requirements Rationale

266 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the Security Assurance Requirements Rationale of the Protection Profiles without repeating these here.

6.3.4 Security Requirements – Internal Consistency

267 This security target claims strict conformance to the Protection Profiles given in section 19. Therefore this security target includes the analysis of the internal consistency of the Security Requirements of the Protection Profiles without repeating these here.

268 As the complete Security Problem Definition, the Extended Components and the Security Functional Requirements have also been included, the consistency analysis of the Protection Profiles is also valid for this security target.

269 The additions made to include the Active Authentication Mechanism have been integrated in a consistent way to the model designed by the Protection Profiles, e. g. by using the subject, object and operation definitions.

270 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 sections 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

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

7.1 TOE Security functions

7.1.1 TSF.AccessControl

272 The TOE provides access control mechanisms that allow the maintenance of different security roles according to FMT_SMR.1/PACE Security roles (Manufacturer, Personalisation Agent, Terminal, PACE authenticated BIS-PACE, Country Verifying Certification Authority, Document Verifier, Domestic Extended Inspection System, Foreign Extended Inspection System).

273 Manufacturer role:

The TOE restricts the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. Manufacturer is the only role with the capability to store the IC Identification Data in the audit records. Users of role Manufacturer are assumed default users by the TOE during the Phase 2.

The TSF.AccessControl provides that the Manufacturer role is only valid in Pre-personalisation of OS according to [7].1.3.2 TOE Life Cycle.

274 Personalisation Agent role:

Personalisation Agent is the only role with the ability:

- to disable read access for users to the Initialisation Data.
- to write the initial CVCA Public Key, the initial CVCA Certificate, and the initial Current Date.
- to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical travel document after successful authentication (until the end of the Personalisation Phase).
- to read out the Initialisation Data and the Pre-personalisation Data.

The Personalisation Agent has the ability to create or load the Chip Authentication Private Key.

The TSF.AccessControl provides that the Personalisation Agent role is only valid in Personalisation phase of IDentity Applet life cycle.

275 Country Verifying Certification Authority role:

The access control mechanisms ensure that only the Country Verifying Certification Authority has the ability to update:

- the CVCA Public Key
- the CVCA Certificate.

CVCA Public Key and CVCA Certificates attributes are updated by the applet.

The CVCA public key is stored by the Platform, attributes are stored by the Applet.

CVCA has the ability to modify the Current Date.

A terminal authenticated as CVCA is explicitly denied reading data in the EF.DG3 and EF.DG4.

The TSF.AccessControl provides that the Country Verifying Certification Authority role is only valid in Operational phase of IDentity Applet life cycle.

276 Document Verifier role:

A terminal authenticated as DV is explicitly denied reading data in the EF.DG3 and EF.DG4.

DV has the ability to modify the Current Date.

The TSF.AccessControl provides that the Document Verifier role is only valid in Operational phase of IDentity Applet life cycle.

277 Terminal role:

A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface. Terminal used by the border control officer is Inspection System.

PACE authenticated Inspection System is the PACE authenticated BIS-PACE. Inspection system which successful implements the terminal and chip authentication (EAC1) gains the role of Foreign or Domestic Extended Inspection System, Country Verifying Certification Authority or Document Verifier. It depends on the value of Inspection System Certificate values.

The TSF.AccessControl provides that the Terminal role is only valid in Operational phase of IDentity Applet life cycle.

278 PACE authenticated BIS-PACE:

PACE authenticated BIS-PACE has the ability after a successful PACE authentication to read out data from EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM (except EF.DG3 and EF.DG4).

The TSF.AccessControl provides that the Basic Inspection System role is only valid in Operational phase of IDentity Applet life cycle.

279 Extended Inspection System role:

The TSF.AccessControl ensures that the Extended Inspection System has the same ability as PACE authenticated BIS-PACE. Furthermore only authenticated (Domestic or Foreign) Extended Inspection System has Read access to:

- DG 3 (Fingerprint) is allowed to read the data in EF.DG3 of the logical travel document.
- DG 4 (Iris) is allowed to read the data in EF.DG4 of the logical travel document.

Domestic Extended Inspection System (but not Foreign EIS) has the ability to modify the Current Date.

In these cases the TOE uses EAC1, which is not used in any other case. In all other cases, reading any of the EF.DG3 to EF.DG4 of the logical travel document is explicitly denied.

The TSF provides that the Extended Inspection System role is only valid in Operational phase of IDentity Applet life cycle.

280 The TSF.AccessControl ensures that nobody is allowed to read all TOE intrinsic secret cryptographic keys stored in the travel document, such as PACE passwords, Chip Authentication Private Key, the Personalisation Agent Keys, and the Active Authentication Private Key.

281 Any terminal is explicitly denied modifying any of the EF.DG1 to EF.DG16 of the logical travel document in operational phase.

282 Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control. Verification of certificate chain is managed by the Applet.

283 The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

284 All security attributes under access control are modified in a secure way so that no unauthorised modifications are possible.

285 The TSF provides functionality for the following SFRs:

FDP_ACC.1/TRM: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl.

FDP_ACF.1/TRM: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FIA_AFL.1/PACE: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF.Authenticate and TSF.AccessControl.

FIA_UAU.1/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.AccessControl.

FIA_UID.1/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.AccessControl.

FMT_MTD.1/AAPK: This requirement is about restriction of the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities

FMT_MTD.1/CAPK: This requirement is about restriction of the ability to create or load the Chip Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The key management is provided by TSF.SecureManagement

FMT_MTD.1/CVCA_INI: This requirement is about restriction of the ability to write certain data to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CVCA_UPD: This requirement is about restriction of the ability to update the Country Verifying Certification Authority Public Key and the Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/DATE: This requirement is about restriction of the ability to modify the current date to certain roles. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/KEY_READ: This requirement is about restriction of the ability to read out certain passwords and keys to none. It is realized by TSF.AccessControl, and by TSF.SecureManagement.

FMT_MTD.1/PA: This requirement is about restriction of the ability to write the Document Security Object (SO_D) to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and is uses the TSF.SecureManagement functionalities.

FMT_SMR.1/PACE Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

7.1.2 TSF.Authenticate

286 After activation or reset of the TOE no user is authenticated.

287 TSF-mediated actions on behalf of a user require the user's prior successful identification and authentication.

288 The Platform contains a deterministic random number generator rated DRG.3 (high) according to AIS20 [20] that provides random numbers used for the authentication.

289 Proving the identity of the TOE is supported by the following means:

- PACE protocol;
- Passive Authentication Mechanism.

290 Proving the genuineness of the TOE is supported by the following means:

- PACE – Chip Authentication Mapping;
- Chip Authentication Protocol v1;
- Active Authentication Mechanism.

291 The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol;
- Symmetric Authentication Mechanism based on AES or TDES;
- PACE protocol
- Active Authentication

292 The TOE implements the following authentication mechanism:

- Symmetric Authentication Mechanism;
- PACE GM and PACE-CAM
- Active Authentication;
- Chip Authentication;
- Terminal Authentication.

293 **Symmetric Authentication Mechanism**

In the Personalisation Phase of the TOE life cycle the TSF.Authenticate enforces to the Personalisation Agent authenticates itself to the TOE by usage of the Personalisation Agent Keys with the following Symmetric Authentication Mechanism.

The Symmetric Authentication mechanism has role in the Personalisation phase, when the TSF data for PACE are not available (MRZ or CAN).

294 **PACE**

The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and explicit password-based authentication of the TOE and the Terminal. The two main advantages of PACE protocol:

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

The PACE uses the CAN or MRZ, which are not effectively represent secrets, but are restricted revealable.

TSF.Authenticate provides after successful run of PACE protocol the secure messaging (confidentiality, integrity and authenticity of communication) and the Terminal gains the BIS-PACE role.

The PACE-CAM combines PACE and Chip Authentication into one protocol, which allows faster execution than the separates protocol. As a result PACE-CAM provides the advantages of Chip Authentication and PACE as well.

295 **Active Authentication**

TSF.Authenticate is able to Active Authentication Mechanism, which is an alternative to the Chip Authentication for proof the genuineness the TOE (this security feature prevents cloning the TOE).

Active Authentication is based on a challenge-response protocol which proves the knowledge of the Active Authentication Private Key of the TOE.

The Active Authentication Key Pair is a chip individual key pair, which contains:

- Active Authentication Public Key stored in EF.DG15 and signed by Document Signer (proofed the authenticity by passive authentication). The signature is in Documents Security Objects.
- Active Authentication Private Key stored in the secure memory (provided by the Platform) of the TOE.

Prerequisites of the Active Authentication are the following:

- Successful PACE and Passive Authentication.

Active Authentication is not mandatory, but optional.

296 **Chip Authentication**

The Chip Authentication based on an ephemeral-static Diffie-Hellman key agreement protocol so provides secure communication and unilateral authentication of the TOE.

After successful Chip Authentication Secure Messaging is established between TOE and BIS-PACE based on a static key pair (Chip Authentication Key Pair) stored on the TOE.

Advantages of Chip Authentication are the following:

- Proofing the genuineness the TOE;
- Also provides strong session keys for secure messaging.

The Chip Authentication Key Pair is a chip individual key pair, which contains:

- Chip Authentication Public Key stored in EF.DG14 and signed by Document Signer (proofed the authenticity by Passive Authentication). The signature is in Documents Security Objects.
- Chip Authentication Private Key stored in the secure memory (provided by the Platform) of the TOE.

After successful of Chip Authentication protocol, the secure messaging (confidentiality, integrity and authenticity of communication) is insured.

Prerequisites of the Chip Authentication are the following:

- Successful PACE (Secure messaging based on PACE) and Passive Authentication.

297 **Terminal Authentication**

The Terminal Authentication is based on a two move challenge-response protocol that provides explicit unilateral authentication of the BIS-PACE.

During the Terminal Authentication, TSF.Authenticate enforces the TOE to verify the Inspection System Certificate and according to the (Terminal Authorisation) Certificate Holder Authorisation the adequate access and rights are provided for the Terminal.

Prerequisite of the Terminal Authentication are the following:

- Successful Chip Authentication (Secure messaging based on Chip Authentication).

298 Protection of user data transmitted from the TOE to the terminal is achieved by means of secure messaging (done by Platform) with encryption and message authentication codes. After Chip Authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay attacks.

299 The TSF provides functionality for the following SFRs:

FDP_ACF.1/TRM: It is a requirement about access control and authentication (for details see the SFR), the access control is provided by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FIA_AFL.1/PACE: This SFR requires a detection of unsuccessful authentication attempts. It is realized by TSF.Authenticate and TSF.AccessControl.

FIA_API.1: The SFR is about Chip Authentication Mechanism which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/AA The SFR is about Active Authentication protocol which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/PACE-CAM The SFR is about PACE- Chip Authentication Mapping which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_UAU.1/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.AccessControl.

FIA_UAU.4/PACE The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF.Authenticate. For fresh random number is generated by the TSF.Platform.

FIA_UAU.5/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate, and TSF.Platform.

FIA_UAU.6/EAC: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.Platform.

FIA_UAU.6/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.Platform.

FIA_UID.1/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate and TSF.AccessControl.

FMT_MTD.1/AAPK: This requirement is about restriction of the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CAPK: This requirement is about restriction of the ability to create or load the Chip Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CVCA_INI: This requirement is about restriction of the ability to write certain data to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CVCA_UPD: This requirement is about restriction of the ability to update the Country Verifying Certification Authority Public Key and the Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/DATE: This requirement is about restriction of the ability to modify the current date to certain roles. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/PA: This requirement is about restriction of the ability to write the Document Security Object (SO_D) to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.3: This requirement is ensuring that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol Version 1. This is realized by TSF.Authenticate.

FMT_SMR.1/PACE Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

FTP_ITC.1/PACE: The requirement is about a separate communication channel which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

7.1.3 TSF.SecureManagement

300 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [15], the TOE life-cycle is additionally subdivided into 7 steps.). Phase 4 – „Operational Use" is different from all prior phases, when the TOE is still in the secure environment and Test Features are available. During start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication.

301 Test features of the TOE are not available for the user in Phase 4. Deploying test features after TOE delivery does not allow User Data to be manipulated, sensitive User Data (EF.DG3 and EF.DG4) to be disclosed, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks.

302 The TSF provides functionality for the following SFRs:

FMT_MTD.1/AAPK: This requirement is about restriction of the ability to create or load the Active Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CAPK: This requirement is about restriction of the ability to create or load the Chip Authentication Private Key to the Manufacturer and the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CVCA_INI: This requirement is about restriction of the ability to write certain data to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/CVCA_UPD: This requirement is about restriction of the ability to update the Country Verifying Certification Authority Public Key and the Country Verifying Certification Authority Certificate to the Country Verifying Certification Authority It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/DATE: This requirement is about restriction of the ability to modify the current date to certain roles. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_MTD.1/KEY_READ: This requirement is about restriction of the ability to read out certain passwords and keys to none. It is realized by TSF.AccessControl, and by TSF.SecureManagement.

FMT_MTD.1/PA: This requirement is about restriction of the ability to write the Document Security Object (SOD) to the Personalisation Agent. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and it uses the TSF.SecureManagement functionalities.

FMT_SMF.1 The requirement is about performable management functions, which is provided by TSF.SecureManagement and partly the TSF.Platform.

7.1.4 TSF.CryptoKey

303 **Key Generation**

The TSF.CryptoKey provide the following key generation methods:

Symmetric Authentication Mechanism:

The Personalisation Agent keys:

- In case of secure messaging (ISO) scenario, by an off-card entity having the SK.PERS key contained, by IDentity instance. SK.PERS is created in the Configuration Phase.

- In case of secure messaging (GP) scenario by an off-card entity having the IDentity instance's associated Security Domain keys, which have to be set unique value for each individual card during the Operating System (JCOP4) pre-personalisation.

Active Authentication

ECC and RSA are supported key generation algorithm by TSF.CryptoKey.

RSA PKCS#1 v2.2, RSA PKCS#1-PSS and ECDSA are supported digital signature creation cryptographic algorithm.

The Active Authentication Private Key is stored in the chip secure memory (provided by TSF.Platform) and the Active Authentication Public Key is stored in EF.DG15 (protected by Passive Authentication).

PACE

Key Agreement Protocol: Diffie-Hellman-Protocol compliant to PKCS#3 and ECDH.

PACE Session keys: AES or 3DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{ENC}).

Chip Authentication:

ECC and RSA are supported Key Generation algorithm by TSF.CryptoKey.

The Chip Authentication Private Key is stored in the chip secure memory (provided by TSF.Platform) and the Chip Authentication Public Key is stored in EF.DG14 (protected by Passive Authentication).

Key Agreement protocol for Chip Authentication session key: Diffie-Hellman key derivation protocol compliant to PKCS#3 and based on an ECDH protocol

Chip Authentication Session Key: TDES and AES.

Terminal Authentication

RSA PKCS#1 v2.2, RSA PKCS#1-PSS and ECDSA are supported digital signature verification cryptographic algorithm.

304 **Key Usage**

The Active Authentication Key Pair and the Chip Authentication Key Pair are unchangeable in the operation phase.

A successfully authenticated Personalisation Agent is allowed to change the Personalisation Agent Keys. The Personalization Agent Keys are stored by the Platform.

The TSF.CryptoKey prevents to reuse ephemeral key pairs and the session keys (PACE and Chip Authentication) by freshly generated random number (provided by TSF.Platform (DRG.3)).

305 **Key Destruction**

The TSF.CryptoKey destroys cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys in a randomized manner (supported by TSF.Platform) as a follows:

- SK.PERS key is automatically destroyed and not available any more in Operational Phase.
- the PACE Session Keys:
  - after detection of an error in verification of the MAC of a received command,
  - after generation of the Chip Authentication Session Key (i.e. successfully performing the Chip Authentication) and changing the secure messaging to the Chip Authentication Session Keys
- the Chip Authentication Session Keys after detection of an error in verification of the MAC of a received command,
- any session keys before starting the communication with the terminal in a new power-on-session.

306 The TSF provides functionality for the following SFR:

FCS_CKM.1/AA_GEN: The SFR requires generation of cryptographic keys (for Active Authentication). It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CA: The SFR requires generation of cryptographic keys (sessions keys for Chip Authentication v1). It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CA_GEN: The SFR requires generation of cryptographic keys (for Chip Authentication v1). It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/DH_PACE: The SFR requires generation of cryptographic keys (session keys for PACE). It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CAM: The SFR requires generation of cryptographic keys (session keys for PACE-CAM). It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.4: Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/PACE_ENC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/PACE_MAC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CA_ENC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CA_MAC Requires the cryptographic operation (MAC computation and verification). It is provided by TSF. TSF.CryptoKey and TSF.Platform.

FCS_COP.1/EMRTD Requires the cryptographic operation digital signature creation for Active Authentication). It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CAM Requires the cryptographic operation for PACE – Chip Authentication mapping. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/SIG_VER: Requires a use of cryptographic operation (digital signature verification for terminal authentication). It is provided by TSF.CryptoKey and TSF.Platform.

FCS_RND.1: Requires use of operation which is provided by TSF.Platform and TSF.CryptoKey.

FDP_RIP.1: The SFR requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of key objects. This is ensured by TSF.CryptoKey and also TSF.Platform.

FIA_API.1: The SFR is about Chip Authentication Mechanism which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/AA The SFR is about Active Authentication protocol which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/PACE-CAM The SFR is about PACE- Chip Authentication Mapping which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FDP_UCT.1/TRM This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FDP_UIT.1/TRM This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FTP_ITC.1/PACE: The requirement is about a separate communication channel which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

7.1.5 TSF.AppletParametersSign

307 During the IDentity Applet life cycle phases after LOADED state the IDentity Applet 3.4/PACE-EAC1/AA becomes the default Application and reaches SELECTABLE state. This phase is called the Initialization phase. During this phase the following steps are carried out:

- Applet configuration;
- File creation (all control parameters);
- Object creation (all control parameters and some usage parameters).

308 Certain configuration and control parameters are signed, and this signature is verified before closing the Initialization phase. Only the unsigned parameters can be changed by the Initializer. This way only those Application Profiles can be applied which are validated by the Developer and conform to the requirements. The Initialization state cannot be finished by reaching the INITIALIZED state, and the Personalization phase cannot be started without successful signature verification.

309 These signatures can be verified during the whole IDentity Applet life-cycle, thus the non-authorized changed become detectable by applying this TSF.

310 The TSF provides functionality for the following SFRs:

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletParametersSign and TSF.Platform.

7.1.6 TSF.Platform

311 TSF.Platform provides the Manucaturer the capability to store the Initialisation and Pre-Personalistion Data in the audit records.

TSF.Platform provide functionalites (such as CryptoLibrary, random number generation, etc.) to the followings:

- generate Active Authentication Key Pair;
- generate Chip Authentication Key Pair;
- generate PACE and Chip Authentication session keys;
- perform PACE and Chip Authentication secure messaging – encryption/decryption and message authenticaton code;
- perform digital signature generation (Active Authentication);
- perform digital singature verification (Terminal authentication);
- provide mechanism to generate random numbers (DRG.3 (high));
- insure that the TOE shall not emit variations in power consumption or timing during command execution in excess of non useful information enabling access to secret data;
- insure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the objects of session keys and ephemeral private key;
- insure that unauthorized are unable to use electrical contacts interface to gain access to secret data;
- preserve a secure state when exposure to operating conditions causing a TOE malfunction or failure is detected during self-tests;
- implements appropriate measures to continuously counter physical manipulation and physical probing;
- run a suite of self-tests to demonstrate the correct operation of the TSF and to verify the integrity of the TSF data and stored TSF executable code.

312 The TSF provides functionality for the following SFRs:

FAU_SAS.1: The SFR requires audit capabilities, which are provided by TSF.Platform.

FCS_CKM.1/AA_GEN: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CA: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CA_GEN: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/DH_PACE,: The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.1/CAM The SFR requires generation of cryptographic keys. It is realized by TSF.CryptoKey, and because it uses Platform functionalities, TSF.Platform.

FCS_CKM.4 :Requires the cryptographic key destruction according to a specified cryptographic method. This is realized by TSF.CryptoKey and it uses the functionalities of TSF.Platform.

FCS_COP.1/PACE_ENC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/PACE_MAC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CA_ENC: Requires the cryptographic operation (encryption and decryption. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CA_MAC Requires the cryptographic operation (MAC computation and verification). It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/EMRTD Requires the cryptographic operation digital signature creation for Active Authentication). It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/CAM Requires the cryptographic operation for PACE – Chip Authentication mapping. It is provided by TSF.CryptoKey and TSF.Platform.

FCS_COP.1/SIG_VER: Requires a use of cryptographic operation (digital signature verification for terminal authentication). It is provided by TSF.CryptoKey and TSF.Platform.

FCS_RND.1: Requires use of operation which is provided by TSF.Platform and TSF.CryptoKey.

FDP_RIP.1: The SFR requires that the TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of key objects. This is ensured by TSF.CryptoKey and also TSF.Platform.

FIA_API.1: The SFR is about Chip Authentication Mechanism which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/AA The SFR is about Active Authentication protocol which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_API.1/PACE-CAM The SFR is about PACE- Chip Authentication Mapping which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_UAU.4/PACE The requirement is about authentication, and prevention of reuse of authentication data. It is realized by TSF.Authenticate. For fresh random number is generated by the TSF.Platform.

FIA_UAU.5/PACE: The requirement is about authentication, and what can be accessed before and after it. It is realized by TSF.Authenticate, and TSF.Platform.

FIA_UAU.6/PACE This requirement is about the reauthentication in the secure messaging and it is provided by the TSF.Authenticate and it uses the functionalities of TSF.Platform.

FIA_UAU.6/EAC This requirement is about the reauthentication in the secure messaging and it is provided by the TSF.Authenticate and it uses the functionalities of TSF.Platform.

FDP_UCT.1/TRM This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FDP_UIT.1/TRM This requirement is about the protection from unauthorised disclosure during the secure messaging. It is provided by the TSF.CryptoKey but it uses the functionalities of TSF.Platform.

FMT_LIM.1 The requirement is about restricting capabilities after TOE delivery, which is provided by TSF.Platform.

FMT_LIM.2 The requirement is about restricting capabilities after TOE delivery, which is provided by TSF.Platform.

FMT_MTD.1/INI_ENA: This requirement is about restriction of the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer. The control before the operational phase is provided by TSF.Platform.

FMT_MTD.1/INI_DIS: This requirement is about restriction of the ability to read out the Initialisation Data and Pre-personalisation Data to the Personalization Agent. The control before the operational phase is provided by TSF.Platform.

FMT_SMF.1 The requirement is about performable management functions, which is provided by TSF.SecureManagement and partly the TSF.Platform.

FMT_SMR.1/PACE Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate and the Manufacturer role is ensured by TSF.Platform.

FPT_EMS.1: Requires use of operation which is provided by TSF.Platform.

FPT_FLS.1: The requirement requires the preservation of a secure state when detecting failures. This is provided by TSF.Platform.

FPT_PHP.3: Requires resistance to physical manipulation and probing to the Platform. This is realized by the TSF.Platform.

FPT_TST.1: Requires self-test and capability to verify integrity of TSF and TSF data. This is provided by TSF.AppletParametersSign and TSF.Platform.

FTP_ITC.1/PACE: The requirement is about a separate communication channel which is provided by TSF.Authenticate, TSF.CryptoKey and TSF.Platform.

FIA_UID.1/PACE The requirement is about timing of the user identification which is provided by TSF.AccessControl, TSF.Authenticate and TSF.Platform.

FIA_UAU.1/PACE The requirement is about timing of the user authentication which is provided by TSF.AccessControl, TSF.Authenticate and TSF.Platform.

7.2 Assurance Measures

313 This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 6.3.

314 The following table lists the Assurance measures and references the corresponding documents describing the measures.

Assurance measures	Description
AM_ADV	The representing of the TSF is described in the documentation for functional specification, in the documentation for TOE design, in the security architecture description and in the documentation for implementation representation.

AM_AGD	The guidance documentation is described in the ID&Trust IDentity Applet Suite v3.4 Administrator's Guide [5] and IDentity Applet v3.4 User's Guide [6].
AM_ALC	The life-cycle support of the TOE during its development and maintenance is described in the life-cycle documentation including configuration management, delivery procedures, development security as well as development tools.
AM_ATE	The testing of the TOE is described in the test documentation.
AM_AVA	The vulnerability assessment for the TOE is described in the vulnerability analysis documentation.

10. Table References of Assurance measures

7.3 Fulfilment of the SFRs

315 The following table shows the mapping of the SFRs to security functions of the TOE.

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FAU_SAS.1	-	-	-	-	-	X
FCS_CKM.1/AA_GEN	-	-	-	X	-	X
FCS_CKM.1/CA	-	-	-	X	-	X
FCS_CKM.1/CA_GEN	-	-	-	X	-	X
FCS_CKM.1/DH_PACE	-	-	-	X	-	X
FCS_CKM.1/CAM	-	-	-	X	-	X
FCS_CKM.4	-	-	-	X	-	X
FCS_COP.1/CA_ENC	-	-	-	X	-	X
FCS_COP.1/CA_MAC	-	-	-	X	-	X
FCS_COP.1/PACE_ENC	-	-	-	X	-	X
FCS_COP.1/PACE_MAC	-	-	-	X	-	X
FCS_COP.1/EMRTD	-	-	-	X	-	X
FCS_COP.1/SIG_VER	-	-	-	X	-	X
FDP_ACC.1/TRM	X	-	-	-	-	-
FCS_COP.1/CAM	-	-	-	X	-	X
FCS_RND.1	-	-	-	X	-	X
FDP_ACF.1/TRM	X	X	-	-	-	-
FDP_RIP.1	-	-	-	X	-	X
FDP_UCT.1/TRM	-	-	-	X	-	X
FDP_UIT.1/TRM	-	-	-	X	-	X
FIA_AFL.1/PACE	X	X	-	-	-	-
FIA_API.1	-	X	-	X	-	X
FIA_API.1/AA	-	X	-	X	-	X
FIA_API.1/PACE-CAM	-	X	-	X	-	X
FIA_UAU.1/PACE	X	X	-	-	-	X
FIA_UAU.4/PACE	-	X	-	-	-	X

TOE SFR / Security Function	TSF.AccessControl	TSF.Authenticate	TSF.SecureManagement	TSF.CryptoKey	TSF.AppletParametersSign	TSF.Platform
FIA_UAU.5/PACE	-	X	-	-	-	X
FIA_UAU.6/EAC	-	X	-	-	-	X
FIA_UAU.6/PACE	-	X	-	-	-	X
FIA_UID.1/PACE	X	X	-	-	-	X
FMT_LIM.1	-	-	-	-	-	X
FMT_LIM.2	-	-	-	-	-	X
FMT_MTD.1/AAPK	X	X	X	-	-	-
FMT_MTD.1/CAPK	X	X	X	-	-	-
FMT_MTD.1/CVCA_INI	X	X	X	-	-	-
FMT_MTD.1/CVCA_UPD	X	X	X	-	-	-
FMT_MTD.1/DATE	X	X	X	-	-	-
FMT_MTD.1/INI_DIS	-	-	-	-	-	X
FMT_MTD.1/INI_ENA	-	-	-	-	-	X
FMT_MTD.1/KEY_READ	X	-	X	-	-	-
FMT_MTD.1/PA	X	X	X	-	-	-
FMT_MTD.3	-	X	-	-	-	-
FMT_SMF.1	-	-	X	-	-	X
FMT_SMR.1/PACE	X	X	-	-	-	X
FPT_EMS.1	-	-	-	-	-	X
FPT_FLS.1	-	-	-	-	-	X
FPT_PHP.3	-	-	-	-	-	X
FPT_TST.1	-	-	-	-	X	X
FTP_ITC.1/PACE	-	X	-	X	-	X

11. Table Mapping of SFRs to mechanisms of TOE

7.4 Correspondence of SFR and TOE mechanisms

316 Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8 Glossary and Acronyms

317 For Glossary and Acronyms please refer to the corresponding section of [17]

9 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

[5] IDentity Applet Suite v3.4 Administrator's Guide

[6] IDentity Applet Suite v3.4 User's Guide

[7] JCOP 4 P71 4 Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.1 – 2021-02-12

[8] Supporting Document Mandatory Technical Document Composite product evaluation for Smart Cards and similar devices; Version 1.5.1, May 2018

[9] BSI TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 eMRTDs with BAC/PACEv2 and EACv1 - Version 2.20 26., February 2015

[10] BSI TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 Protocols for electronic Identification, Authentication and trust Services (eIDAS) - Version 2.21, 21. December 2016

[11] BSI TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 Common Specifications – Version 2.21, 21. December 2016

[12] BSI TR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 4 Applications and Document Profiles – Version 2.21, 21. December 2016

[13] International Civil Aviation Organization (ICAO) Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015

[14] International Civil Aviation Organization (ICAO) Supplemental Access Control for Machine Readable Travel Documents, Version – 1.1, 15. April 2014

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

[16] Protection Profile — Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP), Version 1.10, BSI-CC-PP-0055, 25.03.2009

[17] Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), Version 1.3.2, BSI-CC-PP-0056-V2-2012, 05.12.2012

[18] Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011-MA-01 Version 1.01, 22th July 2014

[19] EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

[20] EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

[21] BSI: Common Criteria Protection Profile - Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087 version 1.01, May 20th, 2015

[22] CEN/TS 15480-2 – Identification card systems - European Citizen Card - Part 2: Logical data structures and card services

[23] European Card for e-Services and National e-ID Applications - IAS ECC, Revision 1.0.1, 21.03.2008

[24] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73

[25] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 2.0 28.06.2012

[27] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., May 2015.

[28] JCOP 4 P71 D321 User manual for JCOP 4 P71 Rev. 3.7 – 20190531

[29] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[30] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, version 1.0, March 8,2016, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[31] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library – Security Target Lite – Rev. 1.8 – 19 January 2021