ID&TRUST DOCUMENTS COMMON CRITERIA EVALUATION

EMRTD WITH PACE-EAC1

01. SECURITY TARGET ID&TRUST IDENTITY CARD 3.2

Revision history

Version	Date	Information
v.0.1.	26.09.2012.	First Draft
v.0.2.	12.10.2012.	First version sent for approval
v.0.3.	16.10.2012.	Second version sent for approval
v.0.4.	18.10.2012.	All comments united – sent for approval
v.0.5.	10.11.2012.	Other comments built in
v.0.6.	28.11.2012.	Changes
v.0.7.	03.12.2012.	Further changes
v.0.8.	09.01.2013.	NXP Version corrected
v.0.9.	24.01.2013.	Minor changes
v.0.10.	14.02.2013.	Minor changes again
v.0.11.	14.02.2013.	New Application notes
v.0.12.	20.02.2013.	Fault corrections
v.0.13	11.04.2013.	Corrections in the Rationales
v.0.14.	31.05.2013.	Corrections
v.0.15.	14.06.2013.	Corrections
v.0.16.	24.06.2013.	Corrections
v.0.17.	08.07.2013.	TOE Conciliation
v.0.18.	10.07.2013.	A new version due to the crash of the word processor.
v.0.19.	06.08.2013.	Revisions changes
v.0.20.	30.08.2013.	Further revision changes
v.0.21.	18.09.2013.	Style and format revisions
v.0.22.	25.09.2013.	Composite TOE considerations
v.0.23.	14.10.2013.	The ETR fc indicated changes
v.0.24.	20.10.2013.	Further changes, Statement of compatibility
v.0.25.	11.11.2013.	Statement of Compatibility further changes
v.0.26.	06.12.2013.	Review, finishing touches

v.0.27.	09.12.2013.	Identity applet 3.0 -> 3.1
v.0.28.	13.01.2014.	Evaluator-induced changes
v.0.29.	21.01.2014.	Platform finalization
v.0.30.	27.01.2014.	Title and title references harmonization
v.0.31.	04.02.2014.	Task assignment to the Platform or Applet
v.0.32.	18.02.2014.	Evaluator-induced corrections
v.0.33.	20.02.2014	Test-related corrections
v.0.34.	18.03.2014.	Name finalisation
v.0.35.	24.03.2014.	Platform reference corrections
v.0.36.	16.01.2015.	Review
v.0.37.	21.01.2015.	New guidance documents, correction of the reference
v.0.38.	13.08.2015.	Huntrust->ID&Trust, Certifier review
v.0.39.	06.01.2016.	IDentity Applet 3.1 -> 3.2
v.0.40.	09.02.2016.	FIA_AFL.1.1/1.2/PACE are updated
v.0.41.	04.03.2016.	Evaluator-induced corrections
v.0.42.	05.03.2016.	TOE reference corrections
v.0.43.	08.03.2016.	Reference corrections

Table of Contents

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" [4] 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 This Technical Report [4] 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.

- States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required.
- 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 [26] contains all the relevant indormations about the methodology to handle such a TOE.The developer followed the direction of the mandatory document, and so should any relevant parties participating in the evaluation and certification of the TOE.

1.1 ST Reference

10 Title: Security Target ID&Trust IDentity Card 3.2.

TOE: ID&Trust IDentity Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite Version 3.2 / PACE-EAC1

TOE short name: IDentity v3.2/PACE-EAC1

Editor(s): Tamás Szabó ID&Trust.

CC Version: 3.1 (Revision 4)

Assurance Level: EAL4 augmented with the following assurance components: AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

Version Number: 0.43

Date: 08.03.2016.

TOE Documentation:

- IDentity Applet Initialization and configuration Version 3.2.07
- IDentity Applet Administrator’s Guide Version 3.2.18
- IDentity Applet User’s Guide Version 3.2.19

1.2 TOE Reference

11 The Security Target refers to the product “ID&Trust IDentity Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite Version 3.2 / PACE-EAC1” (TOE) for CC evaluation.

12 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 EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 under the certificate number C13-37760 [16]

Long platform name: J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65 Secure Smart Card Controller Revision 3

Short name: JCOP 2.4.2 R3

It consists of:

a. Smart card platform (SCP), which consists of:
   - Hardware Abstraction Layer with the Crypto Lybrary,
   - Hardware Platform
b. Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager)
c. Native MIFARE application (physically always present but logical availability depends on configuration)
and

ii. the Application Part of the TOE:
ID&Trust IDentity Applet Suite Version 3.2, configured as eMRTD application,

iii. the associated guidance documentation.

1.3 TOE Overview

13 The Target of Evaluation (TOE) addressed by the current Security Target is the „ID&Trust IDentity Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite Version 3.2 / PACE-EAC1" which is an electronic travel document representing a contactless / contact smart card programmed according to ICAO Technical Report "Supplemental Access Control" [4] (which means amongst others according to the Logical Data Structure (LDS) defined in [6]) and additionally providing the Extended Access Control (EAC) according to the 'ICAO Doc 9303' [6] and BSI TR-03110 [5], 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 [7].

14 The Application part of the TOE, the applet functionalities are distributed according to the following table:

No	Function	Standard
1	European citizen card	CEN/TS 15480-2
2	European card for e-Services and National e-ID applications	IAS-ECC 1.0.1 specification
3	Basic Access Control	ICAO Doc 9303
4	Extended Access Control v1	BSI TR-3110 version 2.10
5	International Driving License	ISO/IEC 18013
6	European Driving License	EC 383/2012

Table 1: Applet functionalities

15 All the functions are supplied by the applet "ID&Trust IDentity Applet Suite Version 3.2", the behaviour of the applet changes according to the environmental behaviour. The scope of the current ST is only concerned with applet behaviour No 3 and No 4, the reasons are explained below.

16 IDentity Card 3.2 can be configured and used for different kind of electronic identity products based on the extended version of the same standard (BSI TR-03110), so called EAC2. While EAC2 was not subject of the CC evaluation, the evaluation was made for the product already having EAC2 support.

Meanwhile, there is a new version of TR-03110 v2.20 where many optional features are standardized. One of these new features is enabling access control for non-standard Data Groups within CV Certificates, so called "Authorization Extensions to be used for local Generic Attributes" (see BSI TR-03110 v2.20 Part 4 sec. 2.2 for the details). This feature is implemented by the new version of ID&Trust IDentity Card applet accordingly. The actual implementation of the change happens in the EAC2 branch of the applet function, so it does not effect the certified functions of the IDentity applet. In order to be separated from the evaluation version, the IDentity Card 3.1 applet is renamed IDentity Card 3.2.

17 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, Extended Access Control, and Chip Authentication similar to the Active Authentication in 'ICAO Doc 9303' [6].

18 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 [7] and [18] 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 [18], [7].

19 For the TOE, beside the eMRTD application other applications may be present on the JCOP 2.4.2 R3. They 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 (certificate number C13-37760), which includes the chip (BSI-DSZ-CC-0858) and the crypto library (BSI-DSZ-CC-0750-V2-2014).

20 Part of the TOE are the associated guidance documentation, the User's Guide, the Administrator's Guide and the Initialization and configuration guides.

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

1.3.1 Non-TOE hardware/software/firmware

22 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

23 The Target of Evaluation (TOE) addressed by the current Security Target is „ID&Trust IDentity Card 3.2: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust IDentity Applet Suite Version 3.2 / PACE-EAC1" which an electronic travel document representing a contactless / contact smart card. For this security target the travel document is 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.

24 ii. the logical travel document as data of the travel document holder stored according to the Logical Data Structure as defined in [6] 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).

25 **Application Note 1 (of the ST author):** The biometric reference data (EF.DG3 and EF.DG4) are optional according to [6]. 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

26 **Integrated Circuit (Smart Card Platform)**

- **Secure Smart card controller including IC dedicated software**
  NXP Secure Smart Card Controllers P5CD145V0v/ V0B(s)and P5CC145V0v/ V0B(s)
  Evaluation Level for the Smart Card Controller: EAL 5 augmented by ASE_TSS.2, AVA_VAN.5 and ALC_DVS.2, claiming conformance to the Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-CC-PP-0035-2007. Certification number: BSI-DSZ-CC-0858
- **Crypto Library**
  Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)
  Evaluation Level for the hardware Platform including the cryptographic library: CC EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5, claiming conformance to the Protection Profile “Bundesamt für Sicherheit in der Informationstechnik (BSI): Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035”. Certification number: BSI-DSZ-CC-0750-V2-2014

Embedded Software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager) and Native MIFARE application

- OS Name: JCOP 2.4.2 R3
- Product Identification: J3E120_M65 / J2E120_M65 / J3E082_M65 / J2E082_M65

Evaluation Level : CC EAL 5+ with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 according to Java Card System – Open Configuration Protection Profile, version 2.6, certified by ANSSI,19.04.2010. Certification number: C13-37760.

IDentity applet – accomplishing IDentity application

Applet name: ID&Trust IDentity Applet Suite

Version: 3.2.

IDentity application – implemented by an application profile.

TOE Guidance Documentation:

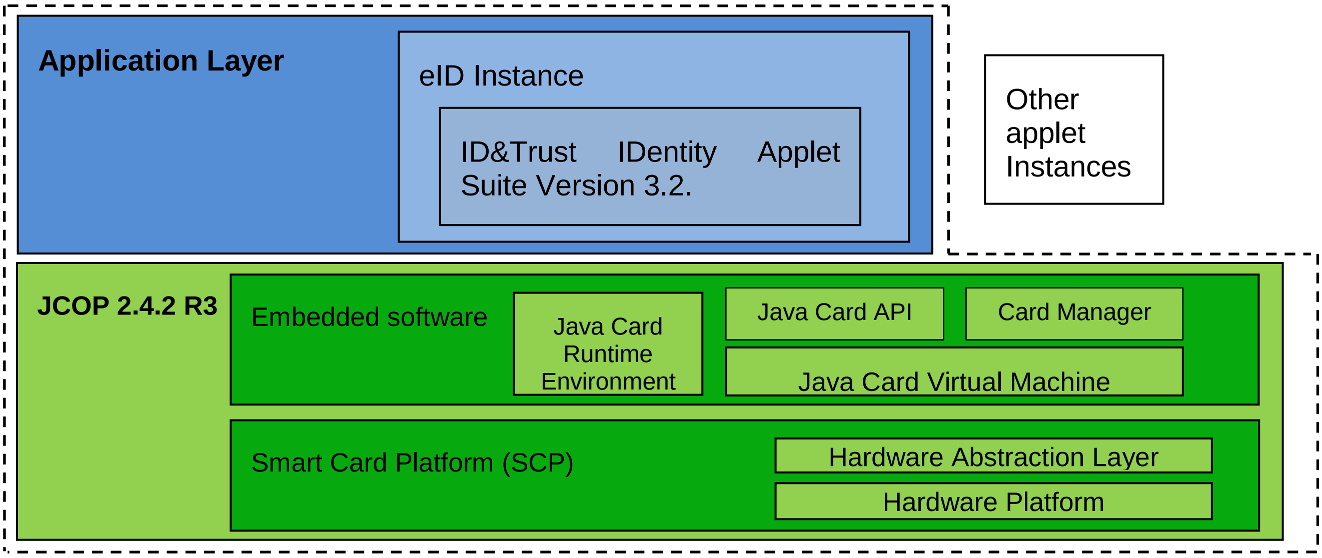
- IDentity Applet Initialization and configuration Version 3.2.07

- IDentity Applet Administrator’s Guide Version 3.2.18

- IDentity Applet User’s Guide Version 3.2.19

The composite part always means ID&Trust IDentity Suite 3.2.

27 The logical architecture of the TOE:


Application Layer
eID Instance
ID&Trust IDentity Applet Suite Version 3.2.
Other applet Instances
JCOP 2.4.2 R3
Embedded software
Java Card Runtime Environment
Java Card API
Card Manager
Java Card Virtual Machine
Smart Card Platform (SCP)
Hardware Abstraction Layer
Hardware Platform

1.4.3 TOE usage and security features for operational use

28 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.

29 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) [6]. These security measures can include the binding of the travel document's chip to the travel document.

30 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.

31 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 [6], and Password Authenticated Connection Establishment [4]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

32 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 [5] as an alternative to the Active Authentication stated in [6].

33 If BAC is supported by the TOE, the travel document has to be evaluated and certified separately. This is due to the fact that [8] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3).

34 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)’ [7]. Note that [7] considers high attack potential.

35 For the PACE protocol according to [4], 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 KMAC and KENC 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) [5], [4].

36 The security target requires the TOE to implement - among others - the Extended Access Control as defin ed in [5]. 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) 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 Protocol authenticates the travel document’s chip to the inspection system.

1.4.4 TOE life cycle

37 The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [9], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

38 Phase 1 “Development”

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

39 (Step2) NXP 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 eMRTD application and the guidance documentation associated with these TOE components are

developed by ID&Trust Ltd.[1]

40 The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software and the eMRTD application 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.

41 Phase 2 “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 eMRTD application. 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.

42 If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM). The IC manufacturer in this phase preconfigures the JCOP card and the EEPROM.

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

44 (Step5) The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM or FLASH) if necessary (this is the so-called Pre-personalization), (ii) creates the eMRTD application, and (iii) equips travel document’s chips with preloaded-personalisation Data.

45 **Application note 2 (redefined for the goals of this ST by the ST author, originally from [18]):** Creation of the application implies the Applet ROM-coding NXP burns the ROM of the integrated circuits putting the IDentity on it. This procedure is called ROM coding. Once it is done, the card or integrated circuit cannot be programmed or reprogrammed again 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 Applet, which are preinstalled by the Travel Document Manufacturer, and which are needed and used in the Personalization process.

46 Phase 3 “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

[1] In the case of the Current Security Target, the Common Criteria Certified JCOP v2.4.2 R3 platforms also the IC Embedded Software (Operating System) and the IC Dedicated Softwarec (cryptographic library) and becasue of ROM coding the eMRTD application, thus the Software Developers are two separated entities, NXP and ID&Trust, the latter only responsible for the development of the IDentity Applet. The development of the platform and the cryptolibrary is at one developer, NXP, the development of the Applet and related documentation is at an another site in Hungary, by ID&trust Ltd. For more information on this, see Statement of Compatibility concerning Composite Security Target chapter.

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.

47 **Application Note 3 (of the ST author):** The referred Personalization Agent can be the card issuer, or a different contributor, depending on the business case, but the intended customer of the TOE is the Card Issuer, who will participate in the process before (until) the *Operational Phase* of the Applet. The 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 IDentity Applet Administrator’s Guide.[23] These states and phases are presented here because of informational reasons, to serve better understanding.
The Phase of Personalization of the TOE Platform and Application Parts are the same. At the end of the phase the developer issues the Finish Configuration command. Part of this command is the verification of the authentic profile. The Personalization Agent Authentication Keys which are loaded at the end of Phase 2 can be changed during this phase by the Personalization Agent

48 The signing of the Document security object by the Document signer [6] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use. This is the end of the Personalization phase.

49 **Application note 4 (taken from [18]):** This security target distinguishes between the Personalisation Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [6]. This approach allows but does not enforce the separation of these roles.

50 Phase 4 “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.

51 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.

52 Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

1.4.5 TOE security functions

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

54 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,

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

56 Averting of inconspicuous tracing of the travel document,

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

58 These are described below informally, and in detail in section 7.1.

1.4.6 Features of the Applet

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

60 IDentity applet may be considered as a highly secure and configurable multi-application cryptographic smart card framework for PKI and e-ID purposes.

61 IDentity applet complies with the standards referenced in TOE Overview.

62 The API exposed by IDentity allows fast development of cryptographic supported applications for National ID, ePassport, Enterprise ID, Healthcare, Transportation, and Payment applications.

63 IDentity 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 5+ both the microprocessor and the JCOP OS as well. JCOP 2.4.2 R3 is protected against state of the art attacks.

64 The OS:

- supports ISO 14443-4 Type A, ISO/IEC 7816-4, 8 and 9 standards

- supports PC/SC applications
- provides fast cryptography
- enforces smart memory management
- provides strong security and data integrity mechanisms

1.4.6.1 File System

65 The applet file system is based on the following basic file types:

- directory files, denoted as Dedicated Files (DF)
- application containers, denoted as Application Dedicated Files (ADF)
- generic data files, denoted as Elementary Files (EF)

66 A Dedicated File (DF) represents a directory and may include other objects (except ADFs). A DF contains a set of information dedicated to control the access to this DF and to its included objects. The supported operations on DFs are: creation, selection and deletion.

67 An Application Dedicated File (ADF) is a special kind of Dedicated File having an ISO/IEC 7816-4 Application Identifier (AID) which represents an application and may include other objects. This ST uses the “smart card application” terminology for ADFs and “applet” terminology for Java Card applets. An ADF contains a set of information dedicated to control the access to this ADF and to its included objects. The supported operations on ADFs are: creation, selection and deletion.

68 Elementary File (EF) is used for data storage. For this reason EFs are also referred to as data files. File access is similar to traditional file systems controlled by access control rules. The IDenity applet supports ISO/IEC 7816-4 transparent EFs only. Transparent files are seen as a single continuous sequence of data units with granularity of one byte. The supported data unit size is one byte. Any data can be accessed by providing an offset and a length. The supported operations on EFs are: read binary, update binary, file selection and deletion. The card is able to import, store and export data in the file system.

69 The Master File (MF) is the root of the file system and is always the initial entry point to the file system. It is implicitly selected after a reset of the card. The MF can be considered to be a special ADF that contains all the files and security data objects.

1.4.6.2 Data Objects

70 A DataObject (DO) represents a byte string available from everywhere in the directory architecture. For example, the serial number is retrieved with this method.

1.4.6.3 Security Data Objects

71 The card manages a security object system allowing management of access conditions, and cryptographic operations. It is implemented using Security Data Objects. There is a particular type of Security Data Object which is the Security Environment saved in EEPROM. They hold the card security policy.

72 During Personalization Phase special built-in security policy – so called Security Policy (perso) – is applied for all objects created and updated.

Security Policy (perso) is defined as the following:

If Protocol configuration byte is ‘00’, Secure Messaging (perso) is not needed.

If Protocol configuration byte is other than ‘00’, Secure Messaging (perso) is needed.

Additionally, there are some built-in security requirements in the Operational phase regardless of the configured security attributes. It is depending on the current ADF life cycle state, see Admin Guide [23] 7.2.

73 A Security Data Object represents a secret or a public part of a secret and is always involved in cryptographic operation. For example a PIN is a Security Data Object.

74 The card is able to import, store and export security data objects being in the security object system.

75 After the IDentity instance life cycle state becomes PERSONALIZED, Security Policy (perso) will not be available any more. Access control will be managed by the applet based on the configured security attributes, so called Security Policy (usage).

1.4.6.4 Security Environments

76 A Security Environment is involved in the card security context setting (clarifying algorithm or Security Data Object to use) when needed dynamically, or to determine the access control rules of an object / file.

77 The TOE is resistant to physical tampering on the TSF. The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

1.4.6.5 Secure Messaging

78 All commands can be secured.

79 Secure Messaging is managed by the Platform, and can be achieved by two different ways during Perso phase:

- Secure Messaging (GP) - GlobalPlatform Secure Messaging
- Secure Messaging (ISO) – ISO Secure Messaging –, established with standard MUTUAL AUTHENTICATE command using the SK.PERS key.

Supports command chaining and extended length APDUs with data length up to 32K bytes More about the Secure Messaging and the key can be read in the Administrator’s Guide document [23]. Additionally Secure Messaging can be achieved also by BAC, PACE, CA during the Operational phase.

1.4.6.6 Memory Management

80 All internal file system structures are stored in highly reliable non-volatile memory with guaranteed data integrity. All memory updates are updated using “atomic operations”. This provides safe operations even when power is interrupted.

81 Content of deleted files and objects are cleared (wiped) and returned to the “free memory pool” for reuse.

1.4.6.7 Access Control

82 The TOE provides access control mechanisms that allow the maintenance of

different users (Manufacturer, Personalisation Agent, Terminal, PACE authenticated BIS-PACE, Country Verifying Certification Authority,Document Verifier, Domestic Extended Inspection System, Foreign Extended Inspection System).

83 The TOE administers the user roles enabling and restricting capabilities and accesses. The access control mechanisms allow the execution of certain security relevant actions (e.g. self-tests) without successful user authentication.

84 Before applet instantiation only the role of the Manufacturer exist, who is responsible for the pre-personalization. After that, the applet instantiation requires the Card Issuer or a dedicated Application Provider Role. After the instantiation, during Personalization, the card is prepared to handle the Personalization Agent and the Application Profile Provider Roles. After Personalization, when the card usage started, the applet does not contain predefined roles for the operational phase, because those are contained by the Application Profile.

More about the Management of roles can be read in the Administrator's Guide document.[23]

85 The access control is administered through authentication mechanisms.

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

- Chip Authentication Protocol
- Active Authentication Mechanism

In these the functions the methods are divided between the Platform and the Applet as follows.

Chip Authentication: Applet: terminal ephemeral public key validation, CA private key permission verification, session counter initialization. Platform: key agreement (DH, ECDH), hashing for session key computation.

Active Authentication: Applet: ISO padding for RSA. Platform: hashing, digital signature

87 The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol
- Symmetric Authentication Mechanism based on AES / Triple DES

In these the functions the methods are divided between the Platform and the Applet as follows.

Terminal Authentication Protocol: Applet: certificate attributes validation. Platform: hashing, signature verification with padding (PKCS, PSS)

Symmetric Authentication Mechanism: Applet: symmetric key permission verification, session counter initialization. Platform: symmetric key cryptography, hashing for session key computation

88 After completion of the PACE Protocol or the Chip Authentication Protocol, the TOE accepts commands with correct message authentication code only. These commands must be send via secure messaging using the key previously agreed with the terminal during the last authentication. More about these functions can be read in section 7.1.

1.4.6.8 Cryptography

89 Counter measures are in operation against state of the art attacks such as SPA/DPA.

90 The TOE supports onboard generation of cryptographic keys based on the DH and ECDH compliant as well as generation of RSA and ECDSA key pairs

91 The TOE supports overwriting the cryptographic keys with zero values as follows:

- the PACE Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol,
- the Chip Authentication Session Keys after detection of an error in a received command by verification of the MAC,

any session keys before starting the communication with the terminal in a new power-on-session.

92 The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [20] that provides random numbers used authentication. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying Platform.

93 The algorithms allowed for the different functions are the following, as is stated in the Users Guide [24]

94 Active Authentication:

- ISO/IEC 9796-2 SHA-1 (Applet: ISO padding for RSA. Platform: hashing, digital signature)
- ISO/IEC 9796-2 SHA-256 (Applet: ISO padding for RSA. Platform: hashing, digital signature)
- ECDSA SHA-1 (All by the Platform)
- ECDSA SHA-224 (All by the Platform)
- ECDSA SHA-256 (All by the Platform)

95 IAS-ECC algorithms:

- PKCS#1 v1.5 SHA-1 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-256 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-384 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v1.5 SHA-512 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-1 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-256 (All by the Platform: padding, hashing, digital signature)
- ISO/IEC 9796-2 SHA-384 (All by the Platform: padding, hashing, digital signature)

- ISO/IEC 9796-2 SHA-512 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v2.1 PSS SHA-1 (All by the Platform: padding, hashing, digital signature)
- PKCS#1 v2.1 PSS SHA-256 (Applet padding)
- ECDSA SHA-1 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-224 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-256 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-384 (All by the Platform: padding, hashing, digital signature)
- ECDSA SHA-512 (All by the Platform: padding, hashing, digital signature)

1.4.6.9 Signed Parameters

96 During the Applet life cycle phases after LOADED state the applet becomes the default Application and reaches SELECTABLE state. This is called the Initialization phase. During this phase the following steps are carryed out:

- Applet configuration
- File creation (all control parameters)

Object creation (all control parameters and some usage parameters)

97 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 can not be finished by reaching the INITIALIZED state, and the Personalization phase can not be started without successful signature verification.

The Administrators Guide [23] 5.2.2. contains more about this topic.

1.4.6.10 Write once behaviour

98 The personalization of certain Data Object Usage Parameters is restricted to write once during the Personalization Phase. This way the value of certain Data Object Usage Parameters can be enforced by the Application Profile (e.g. ‘Algorithm to compulsory use’). Note that after personalization – i.e. the applet is in Operational Phase – write once behaviour is not affective any more.

1.4.6.11 Performance

99 IDentity applet supports T=0 and T=1 protocol in contact mode, with speed of up to 223200 bit/s, and T=CL protocol in contactless mode, with speed up to 848 kbit/s.

1.4.6.12 Secure management of the Applet run

100 The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as well as temporarily stored hash values for data to be signed.

101 The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

1.4.6.13 Platform-ensured security functions

102 The following security function is ensured fully by the platform:

TSF_Audit, which is about detection sensors of the Platform. More about this can be read in 7.1. chapter of this ST.

2 Conformance Claims

2.1 Conformance with the Common Criteria

103 This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation [CC],

- Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, [1]
- Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012,[2]
- Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [3]

as follows

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

104 The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012, [10]

has to be taken into account.

2.2 Protection Profile Claim

105 This ST claims strict conformance to the following Protection Profiles:

- Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.1 BSI-CC-PP-0056-V2-2012. [18]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.0 BSI-CC-PP-0068-V2-2011 [7]

2.3 Package Claim

106 The current ST is conformant to the following security requirements package:

- 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

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

108 This ST is conformant with Common Criteria Part 2 [2] extended due to additional components as stated in Protection Profiles BSI-CC-PP-0056-V2-2012 [18] and BSI-

CC-PP-0068-V2-2011 [7].

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

110 The current ST refines the Assets, threats, objectives and SFRs BSI-CC-PP-0056-V2-2012 [18] and BSI-CC-PP-0068-V2-2011 [7].

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

- Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE (EAC PP), version 1.3.1 BSI-CC-PP-0056-V2-2012. [18]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.0 BSI-CC-PP-0068-V2-2011 [7]

112 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” [4].

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

BSI-CC-PP-0056-V2-2012 [18]:

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 [7]:

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

113 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. There is one added assumption, **A.Sec_Manufac**. It does not affect the strict conformance.

114 The **security objectives** of 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 is one security objective added, OT.Active_Auth_Proof (Proof of travel document’s chip authenticity). This security objective do not affect the strict conformance.

115 The **security objectives** for the operational environment in this security target include all security objectives for the operational environment from the PPs. There are two objectives added, OE.Active_Auth_Key_Travel_Document (Travel document Active Authentication Key) and OE.Sec_Manufac (Protection during ROM-coding, Packaging, Finishing and Personalization)**.** These security objectives do not affect the strict conformance.

116 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. There are the following SFRs added in this security target: FCS_CKM.1/AA_GEN**,** FCS_CKM.1/CA_GEN**,** FIA_API.1/AA and FMT_MTD.1/AAPK. Two exisiting SFRs were extended for the inclusion of the Active Authentication private key. FMT_MTD.1/KEY_READ, and FPT_EMS.1.

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

2.5 Statement of compatibility

2.5.1 Security Functionalities

117 The following table contains the security functionalities of the Platform ST and of this ST, showing which Functionality correspond to the platform ST and which has no corresspondence. This statement is compliant to the requirements of [16].

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

Platform Security Functionality	Corresponding TOE Security Functionality	Relevant	Not relevant	Remarks
SF.AccessControl	TSF_AccessControl	X		enforces the access control
SF.Audit	TSF_Audit_MRTD	X		Audit functionality
SF.CryptoKey	TSF_CryptoKey_MRTD	X		Cryptographic key management
SF.CryptoOperation	TSF_Platform, TSF_AppletParameters_Sign	X		Cryptographic operation Used by calling Platform Security Functionalities
SF.I&A	TSF_Authenticate	X		Identification and authentication
SF.SecureManagement	SF_SecureManagement_MRTD	X		Secure management of TOE resources
SF.PIN	TSF_AccessControl	X		PIN management Used by calling Access Control TSF
SF.LoadIntegrity	-		X	Package integrity check
SF.Transaction			X	Transaction management
SF.Hardware	TSF_Platform	X		TSF of the underlying Platform Used by calling Platform Security Functionalities
SF.CryptoLib	TSF_Platform	X		TSF of the certified crypto library Used by calling

				Platform Security Functionalities

Table 2 Classification of Platform-TSFs

119 All listed TSFs of the Platform-ST are relevant for this ST.

120 **Application note 5 (by the ST author)** The TSF_Platform Security functionality in the above list represents functionalities which are not directly used in the IDentity Applet, they are implicitly invoked by calls to the platform, respectively the JCOP operating system. These functions are called altogether as TSF_Platform.

2.5.1.1 Threats

121 The following threats of this ST are directly related to JCOP Platform functionality:

- T.Phys-Tamper
- T.Malfunction
- T.Forgery

122 These threats will be mapped to the following Platform-ST threats:

- T.PHYSICAL
- T.RND
- T.RESOURCES
- T.SID.1

123 The following table shows the mapping of the threats.

This ST		T.Phys-Tamper	T.Malfunction	T.Forgery
Platform ST	T.PHYSICAL	X		
	T.RND		X	
	T.RESOURCES		X	
	T.SID.1			X

Table 3 Mapping of Threats

124 The T.Phys-Tamper matches to T.PHYSICAL, as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

125 The T.Malfunction matches T.RND and T.RESOURCES because these are the threats which may lead to a malfunction of the hardware or the Embedded Software by applying environmental stress in order to deactivate or modify security features or functionality of the TOE hardware or to circumvent, deactivate or modify security functions of the TOE's Embedded Software.

126 T.Abuse-Func matches T.INSTALL as security violations either accidentally or deliberately could access restricted data (which may include code) or privilege levels.

127 T.Forgery matches T.SID.1 because if an attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the inspection system then the impersonation of an another application from T.SID.1 could be relevant.

128 The following threats:

- T.INTEG-APPLI-CODE.LOAD
- T.INTEG-APPLI-DATA
- T.INTEG-APPLI-DATA.LOAD
- T.CONFID-JCS-CODE
- T.CONFID-JCS-DATA
- T.DELETION
- T.EXE-CODE.1
- T.EXE-CODE.2
- T.EXE-CODE-REMOTE
- T.INTEG-APPLI-CODE
- T.INTEG-JCS-CODE
- T.INTEG-JCS-DATA
- T.NATIVE
- T.OBJ-DELETION

- T.SID.2
- T.SEC_BOX_BORDER
- T.OS_OPERATE
- T.CONFID-APPLI-DATA
- T.INSTALL

have no corresponde to the treaths of this ST. They are assessed, and found that there is also no contradiction related to this ST.

2.5.2 OSPS

129 None of the OSPs of this ST are applicable to the JCOP Platform and therefore not mappable for the Platform-ST.

130 The OSP-s from the Platform ST OSP.VERIFICATION and OSP.PROCESS-TOE does not deal with any additional security components.

2.5.3 Assumptions

131 The Assumptions of the Platform ST are categorized according to the [26], as IrPA, CfPA and SgPA. There is also a comment column with respective remarks.

Assumption	Classification of assumptions	Comment
A.APPLET	CfPA	The Java Card specification explicitly "does not include support for native methods" ([28], §3.3) outside the API.
A.VERIFICATION	CfPA	The fulfillment of the assumption is connected to the Life-cycle of the TOE, the Applet is loaded on the ROM by the manufacturer. The assumption A.Sec_Manufac and the related objective OE.Sec_Manufac covers this assumption.
A.USE_DIAG	SgPa	A.Insp_Sys, A_Auth_PKI and the related OE.Prot_Logical_Travel_Document, and OE.Ext_Insp_Systems provide the necessary ensurance.
A.USE_KEYS	CfPA	The Assumption A.Auth_PKI , the policy P.Terminal and the related objectives OE.Ext_Insp_Systems, OE.Authoriz_Sens_Data and OE.Terminal covers this assumption.
A.PROCESS-SEC-IC	SgPA	The assumption A.Sec_Manufac and the related objective OE.Sec_Manufac covers this assumption.

Table 4 Mapping of assumptions

132 A.Sec_Manufac of this ST is included to assume that the Platform arrives to the user with correctly working functions. This have no contradiction to the Platform ST.

2.5.4 Security objectives

133 These Platform-ST objectives can be mapped to this STs objectives as shown in the following table.

Objective from the Platform ST	Objective from this ST
OT.IDENTIFICATION	OT.Identification
OT.OPERATE	OT.Prot_Malfunction
OT.CIPHER	OT.Sens_Data_Conf
OT.SCP.IC	OT.Prot_Phys-Tamper
OT.RND	OT.Prot_Malfunction, OT.Prot_Inf_Leak
OT.TRANSACTION	OT.Prot_Inf_Leak
OT.KEY-MNGT	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality ,OT.Identification, OT.Prot_Inf_Leak
OT.PIN-MGMT	OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality

Table 5 Mapping of security objectives for the TOE

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

- OT.NATIVE
- OT.REMOTE
- OT.OBJ-DELETION
- OT.DELETION
- OT.SEC_BOX_FW
- OT.GLOBAL_ARRAYS_INTEG
- OT.GLOBAL_ARRAYS_CONFID
- OT.REALLOCATION
- OT.RESOURCES
- OT.ALARM
- OT.MF_FW
- OT.LOAD
- OT.SCP.SUPPORT
- OT.SID
- OT.FIREWALL
- OT.INSTALL
- OT.CARD-MANAGEMENT
- OT.SCP.RECOVERY
- OT.EXT-MEM

cannot be mapped because these are out of scope.

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

Objective from the Platform ST	Objective from this ST
OE.USE_DIAG	OE.Ext_Insp_Systems, OE.Passive_Auth_Sign OE.Terminal, OE.Auth_Key_Travel_Document

OE.USE_KEYS	OE.Ext_Insp_Systems, OE.Passive_Auth_Sign OE.Terminal, OE.Auth_Key_Travel_Document
OE.PROCESS_SEC_IC	OE.Personalisation
OE.APPLET	OT.Data_Integrity, OT.Prot_Abuse-Func and OT.Prot_Malfunction
OE.VERIFICATION	OE.Sec_Manufac, OT.Data_Authenticity and OT.Prot_Malfunction

Table 6 Mapping of security objectives of the environment

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

2.5.5 Security requirements

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

Platform SFR	Corresponding TOE SFR	Remarks
FDP_ACC.2/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFC.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1.1/OBJECTS	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.2/FIREWALL_JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/JCVM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.1	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/CA_GEN, FCS_CKM.1/AA_GEN	The FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/CA_GEN, FCS_CKM.1/AA_GEN corresponds to the FCS_CKM.1 requirement of the

		Platform since they contain overlapping requirements.
FCS_CKM.2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.3	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirements are equivalent (physically overwriting the keys with zeros).
FCS_COP.1	FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC , FCS_COP.1/CA_MAC, FCS_COP.1/SIG_VER, FCS_COP.1/RSA_EMRTD	FCS_COP.1 of the Platform matches the equivalent SFRs of the Platform.
FDP_RIP.1/ABORT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/APDU	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/bArray	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/KEYS	FDP_RIP.1	FDP_RIP.1 matches the equivalent SFR of the Platform-ST.
FDP_RIP.1/TRANSIENT	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ROL.1/FIREWALL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_ARP.1	FPT_PHP.3	The Security Alarms requirement FAU_ARP.1 of the Platform corresponds to the FPT_PHP.3 of this ST about physical resistance.
FDP_SDI.2	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPR_UNO.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1	FPT_FLS.1	FPT_FLS.1 matches to the equivalent SFR of the Platform-ST.
FPT_TDC.1	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_ATD.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.2/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_USB.1/AID	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MTD.1/JCRE	No Correspondence	Out of scope (Platform functionality)

		No contradiction to this ST
MT_MTD.3/JCRE	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ITC.2/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_RCV.3/Installer	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ADEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.2.2/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/JCRMI	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_RIP.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/ODEL	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FCO_NRO.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFC.2/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_IFF.1/CM	No Correspondence	Out of scope (Platform functionality)

		No contradiction to this ST
FDP_UIT.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_UID.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMR.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FTP_ITC.1/CM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/EXT_MEM	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_FLS.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FRU_FLT.2/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FPT_PHP.3/SCP	FPT_PHP.3	The FPT_PHP.3 of this ST matches the FPT_PHP.3/SCP of the Platform ST.
FDP_ACC.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SCP	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/LifeCycle	No Correspondence	Out of scope (Platform functionality)

		No contradiction to this ST
FMT_MSA.3/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FIA_AFL.1/PIN	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FTP_ITC.1/LifeCycle	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FAU_SAS.1/SCP	FAU_SAS.1	FAU_SAS.1 of this ST matches to the equivalent SFR of the Platform-ST.
FCS_RNG.1	FCS_RND.1	FCS_RND.1 of the ST matches FCS_RNG.1 of the Platform-ST when the hardware random number generator is used by the TOE.
FCS_RNG.1/RNG2	FCS_RND.1	FCS_RND.1 of the ST matches FCS_RNG.1/RNG2 of the Platform-ST when the hardware random number generator is used by the TOE.
FPT_EMSEC.1	FPT_EMS.1	FPT_EMS.1 matches the FPT_EMSEC.1 of the Platform-ST
FDP_ACC.2/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FDP_ACF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.3/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_MSA.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST
FMT_SMF.1/SecureBox	No Correspondence	Out of scope (Platform functionality) No contradiction to this ST

Table 7 Mapping of Security requirements

2.5.6 Assurance requirements

138 This ST requires EAL 4 according to Common Criteria V3.1 R4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

139 The Platform-ST requires EAL 5 according to Common Criteria V3.1 R4 augmented by: ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2.

140 As EAL 5 covers all assurance requirements of EAL 4 all non augmented parts of this ST will match to the Platform-ST assurance requirements.

2.6 Analysis

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

3 Security Problem Definition

142 This security target 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.

143 The Assets included from the Protection Profiles:

- user data stored on the TOE Primary Asset from [7]
- user data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE) Primary Asset from [7]
- travel document tracing data from Primary Asset [7]
- Accessibility to the TOE functions and data only for authorised subjects Secondary Asset from [7]
- Genuineness of the TOE Secondary Asset from [7]
- TOE internal secret cryptographic keys cryptographic material Secondary Asset from [7]
- TOE internal non-secret cryptographic material from [7]
- travel document communication establishment authorisation data Secondary Asset from [7]
- Logical travel document sensitive User Data from [18]
- Authenticity of the travel document’s chip from [18]

144 Subjects included from the Protection Profiles:

- travel document holder from [7]
- travel document presenter (traveller) from [7]
- Terminal from [7]
- Basic Inspection System with PACE (BIS-PACE) from [7]
- Document Signer (DS) from [7]
- Country Signing Certification Authority (CSCA) from [7]
- Personalisation Agent from [7]
- Manufacturer from [7]
- Attacker from [7]
- Country Verifying Certification Authority from [18]
- Document Verifier from [18]
- Terminal from [18]
- Inspection system (IS) from [18]
- Attacker from [18]

145 The Assumptions included from the Protection Profiles are:

- A.Passive_Auth from [7]
- A.Insp_Sys from [18]
- A.Auth_PKI from [18]

146 The ST contains another Assumption, not in defined in the PPs, justified by the fact that the TOE is divided to two parts. The TOE Part I according to 1.4. is developed by NXP at the NXP sites, which are already certified at the EAL5+ assurance level.

147 ***A.Sec_Manufac Protection during ROM-coding, Packaging, Finishing and Personalization***

It is assumed that security procedures are used correctly by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

148 The Threats included from the Protection Profiles are:

- T.Skimming from [7]
- T.Eavesdropping from [7]
- T.Tracing from [7]
- T.Forgery from [7]
- T.Abuse-Func from [7]
- T.Information_Leakage from [7]
- T.Phys-Tamper from [7]
- T.Malfunction from [7]
- T.Read_Sensitive_Data from [18]
- T.Counterfeit from [18]

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

- P.Manufact from [7]
- P.Pre-Operational from [7]
- P.Card_PKI from [7]
- P.Trustworthy_PKI from [7]
- P.Terminal from [7]
- P.Sensitive_Data from [18]
- P.Personalisation from [18]

150 **Application Note 7 (of 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

151 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.

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

- OT.Data_Integrity from [7]
- OT.Data_Authenticity from [7]
- OT.Data_Confidentiality from [7]
- OT.Tracing from [7]
- OT.Prot_Abuse-Func from [7]
- OT.Prot_Inf_Leak from [7]
- OT.Prot_Phys-Tamper from [7]
- OT.Prot_Malfunction from [7]
- OT.Identification from [7]
- OT.AC_Pers from [7]
- OT.Sens_Data_Conf from [18]
- OT.Chip_Auth_Proof from [18]

153 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 travel document's chip authenticity

The TOE shall support the Basic Inspection Systems to verify the identity and authenticityof the travel document's chip as issued by the identified issuing State or Organisation bymeans of the Active Authentication as defined in [6]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

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

- OE.Legislative_Compliance from [7]
- OE.Passive_Auth_Sign from [7]
- OE.Personalisation from [7]
- OE.Terminal from [7]
- OE.Travel_Document_Holder from [7]
- OE.Auth_Key_Travel_Document from [18]
- OE.Authoriz_Sens_Data from [18]
- OE.Exam_Travel_Document from [18]
- OE.Prot_Logical_Travel_Document from [18]
- OE.Ext_Insp_Systems from [18]

155 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, and the Assumptions about the Platform: .

156 ***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 certification of the Active Authentication Public Key by means of the Document Security Object.

157 **Application Note 8 (of the ST author):** Active Authentication Mechansim is an alternative to the Chip Authentication for identifying the TOE.

158 *OE.Sec_Manufac* ***Protection during ROM-coding, Packaging, Finishing and Personalization***

An Environmental Objective is that security procedures are used correctly by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

4.1 Security Objective Rationale

159 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.

160 In addition to the rationale given by the Protection Profiles, the threat **T.Counterfeit** "Conterfeit 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 Public Active Authentication Key has to be written into EF.DG15 and signed by means of Documents Security Objects as demanded by **OE.Active_Auth_Key_Travel_Document** "Travel Document Active Authentication Key".

161 Also adding to the rationale the additional assumption (**A.Sec_Manufac**) cover the periods of the lifecycle of the TOE where it is in the influence of the Manufacturer, NXP. The **A.Sec_Manufac** assumption can be mapped to the respective objective **OE.Sec_Manufac**.

5 Extended Components Definition

162 This security target claims strict conformance to the Protection Profile [7] given in section 2.2. Therefore this security target includes the definition of all Extended Components from the Protection Profiles without repeating these here.

163 The Extended Components included from the Protection Profiles are:

- FIA_API from [18]
- FAU_SAS from [7]
- FCS_RND from [7]
- FMT_LIM from [7]
- FPT_EMS from [7]

6 Security Requirements

164 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.

165 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.

166 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.

167 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.

168 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.

169 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.

170 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 [6].
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	The Active Authentication Private Key (KPr_{AA}) is used by the

Name	Data
PrivateKey (KPrAA)	TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

Table 8: Additionally defined objects in this ST

6.1 Security Functional Requirements for the TOE

171 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 [7])

172 Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]: not fulfilled, but justified.

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

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

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to [13][2,3] and specified cryptographic key sizes 192, 224, 256 and 320 bits[4] that meet the following: [4].[5]

173 **Application note 9 (of the ST author):** The TOE generates a shared secret value *K* with the terminal during the PACE protocol, see [4]. This protocol is based on the ECDH compliant to TR-03111 [13] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [4] and [13] for details). The shared secret value *K* is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [4] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

174 **Application note 10 (taken from [7])***:* FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [4].

[2] [selection: *Diffie- Hellman-Protocol compliant to PKCS#3, ECDH compliant to [13]*]
[3] [assignment: *cryptographic key generation algorithm*]
[4] [assignment: *cryptographic key sizes*]
[5] [assignment: *list of standards*]

FCS_CKM.1/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys (taken from [18])

175 Hierarchical to: No other components.

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

and FCS_CKM.4 Cryptographic key destruction: fulfilled by 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 an ECDH protocol compliant to ISO 15946[6,7] and specified cryptographic key sizes Triple DES 112 bits, AES 128 bits, 192 bits and 256 bits[8] that meet the following: based on an ECDH protocol compliant to [13].[9]

176 **Application Note 11 (taken from [18]):** FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [5].

177 **Application Note 12 (taken from [18]):** The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Protocol Version 1, see [5]. This protocol is based on the ECDH compliant to TR-03110 (i.e. an elliptic curve cryptography algorithm) (cf. [13] 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 [5]).

178 **Application Note 13 (taken from [18] redefined)**: 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. [5] for the details)

FCS_CKM.1/CA_GEN Cryptographic key generation – Chip Authentication key

179 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/ST.

FCS_CKM.4 Cryptographic key destruction: not

[6] [selection: *based on the key Diffie-Hellman key derivation protocol compliant to PKCS#3, based on an ECDH protocol compliant to ISO 15946*]
[7] [assignment: *cryptographic key generation algorithm*]
[8] [assignment*: cryptographic key sizes*]
[9] [selection: *based on the Diffie-Hellman key derivation protocol compliant to [13] and [5], based on an ECDH protocol compliant to [13]*]

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 ECDSAKeyGen[10] and specified cryptographic key sizes 192, 224, 256, 320 bits[11] that meet the following: ICAO TR-SAC [4] 4.2.[12]

180 **Application Note 13 (of 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 [18] (see Application Note after FMT_MTD.1/CAPK). 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_CKM.1/AA_GEN Cryptographic key generation – Active Authentication key

181 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 RSAKeyGen[13] and specified cryptographic key sizes 1976-2048 bits[14] that meet the following: [6], chapter 9.2.[15]

182 **Application Note 14 (of the ST author):** The Active Authentication key pair can either be generated in the TOE or imported by the Personalisation Manager (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.

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

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

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

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

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

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

FCS_CKM.4 Cryptographic key destruction – Session keys (taken from [7])

183 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 overwriting the key value with zero values[16] that meets the following: none.[17]

184 **Application Note 15 (of 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 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 [7])

185 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[18] in accordance with a specified cryptographic algorithm AES or Triple DES[19] in CBC mode[20] and cryptographic key sizes AES: 128, 192 or 256 bits; Triple DES: 112[21] bit[22] that meet the following: compliant to [4].[23]

[16] [assignment: *cryptographic key destruction method*]
[17] [assignment: *list of standards*]
[18] [assignment: *list of cryptographic operations*]
[19] [selection: *AES, Triple DES*]
[20] [assignment: *cryptographic algorithm*]
[21] [selection: *112, 128, 192, 256*]
[22] [assignment: *cryptographic key sizes*]
[23] [assignment: *list of standards*]

186 **Application note 16 (taken from [7]):** 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-KEnc).

FCS_COP.1/PACE_MAC Cryptographic operation – MAC (taken from [7])

187 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[24] in accordance with a specified cryptographic algorithm CMAC or Retail-MAC[25,26] and cryptographic key sizes Triple DES: 112 or AES-CMAC: 128, 192 or 256[27] bit[28] that meet the following: compliant to [4].[29]

188 **Application note 17 (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 [18])

189 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

[24] [assignment: *list of cryptographic operations*]
[25] [selection: *CMAC, Retail-MAC*]
[26] [assignment: *cryptographic algorithm*]
[27] [selection: *112, 128, 192, 256*]
[28] [assignment: *cryptographic key sizes*]
[29] [assignment: *list of standards*]

FCS_CKM.1.1/CA_ENC The TSF shall perform secure messaging – encryption and decryption[30] in accordance with a specified cryptographic algorithm AES 128, 192 and 256 bits and Triple DES 112 bits[31,32] that meet the following: ICAO TR-SAC [4], chapter 4.6.[33]

190 **Application Note 18 (taken from [18]):** 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 [18])

191 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/CA_MAC The TSF shall perform secure messaging – message authentication code[34] in accordance with a specified cryptographic algorithm CMAC or Retail-MAC[35] and cryptographic key sizes Triple DES: 112 or AES-CMAC: 128, 192 or 256 bit[36] that meet the following: ICAO TR-SAC [4].[37]

192 **Application Note 19 (taken from [37]):** 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.

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

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document (taken from [18])

193 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[38] in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256[39] and cryptographic key sizes 192-320 bits[40] that meet the following: TR-03111 [13], chapter 4.1.2 using curves from the ICAO TR-SAC [4] 4.2.[41]

194 **Application Note 20 (of 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/RSA_EMRTD Cryptographic operation – Signature generation

195 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]: 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/ RSA_EMRTD The TSF shall perform digital signature generation[42] in accordance with a specified cryptographic algorithm and cryptographic key sizes RSA with SHA-1 and SHA-256 1976-2048 bits[43,44] that meet the following: scheme 1 of ISO/IEC 9796-2:2002 [17], Chapter 8.[45,46]

[38] [assignment: *list of cryptographic operations*]
[39] [assignment: *cryptographic algorithm*]
[40] [assignment: *cryptographic key sizes*]
[41] [assignment: *list of standards*]
[42] [assignment: *list of cryptographic operations*]
[43] [assignment: *cryptographic algorithm*]
[44] [assignment: *cryptographic key sizes*]
[45] According to [6], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.
[46] [assignment: *list of standards*]

196 **Application Note 21 (of 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.

6.1.1.3 Random Number Generation (FCS_RND.1)

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

FCS_RND.1 Quality metric for random numbers (taken from [7])

198 Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that K4 (high) according to AIS20 [20].[47]

199 **Application note 22 (of the ST author):** The TOE generates random numbers used for the authentication protocols e. g. as required by FIA_UAU.4/PACE.

6.1.2 Class FIA Identification and Authentication

200 **Application Note 23 (taken from [18]):** The Table 2 provides an overview of the authentication mechanisms used

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalisation Agents	FIA_UAU.4/PACE
Chip Authenticatication Protocol	FIA_API.1/ST, 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

Table 9: Overview on authentication SFRs

201 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

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

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.

202 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 [7])

203 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][48,49] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.[50]

204 FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been surpassed[51], the TSF shell delay each following authentication attempt until the next successful authentication.[52]

FIA_UID.1/PACE Timing of identification (taken from [18])

205 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 [4],

3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,[53]

4. to carry out the Chip Authentication Protocol Version 1 according to [5],

5. to carry out the Terminal Authentication Protocol Version 1 according to [5].

[48] [assignment: *positive integer number*]

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

[50] [assignment: *list of authentication events*]

[51] [selection: *met ,surpassed*]

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

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

6. <u>to carry out the Active Authentication Mechanism</u>[54]

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

206 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.

207 **Application Note 24 (taken from [18]):** 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 Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

208 **Application Note 25 (taken from [18]):** 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).

209 **Application Note 26 (taken from [18]):** 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 relatedpolicy (policies).

FIA_UAU.1/PACE Timing of authentication (taken from [18])

210 Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/PACE.

FCS_UAU.1/PACE The TSF shall allow

1. to establish the communication channel,

2. carrying out the PACE Protocol according to [4],

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 [5],

6. to carry out the Terminal Authentication Protocol Version 1 according to [5],

7. to carry out the Active Authentication Mechanism[55]

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.

211 **Application Note 27 (taken from [18]):** 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 [18])

212 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 [4],

2. Authentication Mechanism based on AES or Triple DES,[56,57]

3. Terminal Authentication Protocol Version 1 according to [5].

213 **Application Note 28 (of the ST author):** The authentication mechanisms use a

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

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

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

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 requirement. This mechanism equals the BAC algorithm with the difference, that the BAC algorythm bases its computations at the data from MRZ, but during the personalization there is no MRZ yet, so as an anotther 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.*

FIA_UAU.5/PACE Multiple authentication mechanisms (taken from [18])

214 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PACE The TSF shall provide

1. PACE Protocol according to [4],

2. Passive Authentication according to [6],

3. Secure messaging in MAC-ENC mode according to [4],

4. Symmetric Authentication Mechanism based on Triple DES or AES,[58]

5. Terminal Authentication Protocol Version 1 according to [5],[59]

to support user authentication.

215 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*.[60]

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

[58] [selection: *Triple DES, AES or other approved algorithms*]
[59] [assignment: *list of multiple authentication mechanisms*]
[60] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]

	presented during the Chip Authentication Protocol Version 1 and the secure messaging established by the Chip Authentication Protocol Version 1.[61]

216 **Application note 29 (taken from [7]):** 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.

217 **Application Note 30 (of 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 succesful 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.

FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE (taken from [7])

218	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.[62]

219 **Application note 31 (taken from [7]):** The PACE protocol specified in [4] 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 [18])

220	Hierarchical to:	No other components.

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

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.[63]

221 **Application Note 32 (taken from [18]):** The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [6] 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/ST Authentication Proof of Identity (taken from [18])

222 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/ST The TSF shall provide a Chip Authentication Protocol Version 1 according to [5][64] to prove the identity of the TOE.[65]

223 **Application Note 33 (taken from [18]):** The TOE implements the Chip Authentication Mechanism v1 specified in [5]. 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 [6]. 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

224 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA The TSF shall provide the Active Authentication Mechanism according to [6][66] to prove the identity of the TOE.[67]

225 **Application Note 34 (of the ST author):** The SFR FIA_API.1/AA 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

[63] [assignment: *list of conditions under which re-authentication is required*]
[64] [assignment: *authentication mechanism*]
[65] [assignment: *authorized user or role*]
[66] [assignment: *authentication mechanism*]
[67] [assignment: *authorized user or role*]

the claimed Protection Profiles.

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 [18])

226 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[68] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document.[69]

6.1.3.2 Access control functions (FDP_ACF)

FDP_ACF.1/TRM Security attribute based access control (taken from [18])

227 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.

228 FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[70] 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 ,

[68] [assignment: *access control SFP*]
[69] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[70] [assignment: *access control SFP*]

c. data in EF.DG4 of the logical travel document ,

d. all TOE intrinsic secret cryptographic keys stored in the travel document.[71]

3. Security attributes:

a. PACE Authentication,

b. Terminal Authentication Version 1,

c. Authorisation of the Terminal.[72]

229 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 [4] after a successful PACE authentication as required by FIA_UAU.1/PACE.[73]

230 FDP_ACF.1.3/TRM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.[74]

231 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

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

[72] [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*]

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

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

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.[75]

232 **Application note 35 (taken from [18]):** The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [5]. 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.

233 **Application note 36 (taken from [18]):** Please note that the Document Security Object (SO_D) stored in EF.SOD (see [6]) 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 [6].

234 **Application note 37 (taken 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.

235 **Application Note 38 (taken from [18]):** 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 [7])

236 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[76] 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* [77]),[78]

3. none.[79]

[75] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[76] [selection: *allocation of the resource to, deallocation of the resource from*]
[77] according to [4]
[78] [assignment: *list of objects*]
[79] [assignment: *list of objects*].

237 **Application note 39 (taken from [7]):** 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 [7])

238 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_UCT.1.1/TRM The TSF shall enforce the Access Control SFP[80] to be able to transmit and receive[81] 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 [7])

239 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[82] to be able to transmit and receive[83] user data in a manner protected from modification, deletion, insertion and replay[84] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[85] has occurred.

[80] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[81] [selection: *transmit, receive*]
[82] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[83] [selection: *transmit, receive*]
[84] [selection: *modification, deletion, insertion, replay*]
[85] [selection: *modification, deletion, insertion, replay*]

6.1.4 Class FTP Trusted Path/Channels

6.1.4.1 Inter-TSF trusted channel (FTP_ITC)

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

240	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.[86]

241 **Application note 40 (taken from [7]):** 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.

242 **Application note 41 (taken from [7]):** 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.

243 **Application note 42 (taken from [7]):** Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.1.5 Class FAU Security Audit

6.1.5.1 Audit Storage (FAU_SAS)

FAU_SAS.1 Audit storage (taken from [7])

244	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
	FAU_SAS.1.1	The TSF shall provide the Manufacturer[87] with the capability to store the Initialisation and Pre-Personalisation Data[88] in the audit records.

[86] [selection: *modification, deletion, insertion, replay*]

245 **Application Note 43 (taken from [7]):** 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.

6.1.6 Class FMT Security Management

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

6.1.6.1 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

247 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.[89]

6.1.6.2 Security management roles (FMT_SMR)

FMT_SMR.1/PACE Security roles (taken from [18])

248 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,

[87] [assignment: *list of audit information*]
[88] [assignment: *list of management functions to be provided by the TSF*]
[89] [assignment: *list of management functions to be provided by the TSF*]

8. Foreign Extended Inspection System.[90]

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

6.1.6.3 Limited capabilities (FMT_LIM)

FMT_LIM.1Limited capabilities (taken from [18])

250 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, if there is DG3 or DG4 on the card. [91]

FMT_LIM.2 Limited availability (taken from [18])

251 Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities: fulfilled by FMT_LIM.

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, if there is DG3 or DG4 on the card.[92]

[90] [assignment: *the authorised identified roles*]
[91] [assignment: *Limited capability and availability policy*]

252 **Application Note 44 (taken from [18]):** The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.

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

6.1.6.4 Management of TSF data (FMT_MTD)

FMT_MTD.1/CVCA_INI Management of TSF data – Initialisation of CVCA Certificate and Current Date (taken from [18])

254 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[93] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date[94]

to the Personalisation Agent[95]

255 **Application Note 45 (of 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 [18])

256 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[96] the
1. Country Verifying Certification Authority Public

[92] [assignment: *Limited capability and availability policy*]
[93] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[94] [assignment: *list of TSF data*]
[95] [assignment: *the authorised identified roles*]

Key,

2. Country Verifying Certification Authority Certificate[97]

to Country Verifying Certification Authority.[98]

257 **Application Note 46 (taken from [18]):** 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. [5]). 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. [5]).

FMT_MTD.1/DATE Management of TSF data – Current date (taken from [18])

258 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[99] the Current date[100] to

1. Country Verifying Certification Authority,

2. Document Verifier,

3. Domestic Extended Inspection System[101].

259 **Application Note 47 (taken from [18]):** The authorized roles are identified in their certificate (cf. [5]) 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 [5]).

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key (taken from [18])

260 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[102] the Chip Authentication Private Key[103] to the Manufacturer and the Personalisation Agent.[104]

[96] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[97] [assignment: *list of TSF data*]
[98] [assignment: *the authorised identified roles*]
[99] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[100] [assignment: *list of TSF data*]
[101] [assignment: *the authorised identified roles*]

261 **Application Note 48 (of 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.

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation Data (taken from [7])

262 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[105] the Initialisation Data and Pre-personalisation Data[106] to the Manufacturer.[107]

FMT_MTD.1/INI_DIS Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data (taken from [7])

263 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[108] the Initialisation Data and the Pre-personalisation Data[109] to the Personalisation Agent.[110]

264 **Application note 49 (taken from [7]):** 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’.

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

FMT_MTD.1/KEY_READ Management of TSF data – Key Read (taken from [18])

265	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/KEY_READ	The TSF shall restrict the ability to read[111] the 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalisation Agent Keys, 4. Active Authentication Private Key[112] to none.[113]

266 **Application Note 50 (of 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 [7])

267	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[114] the Document Security Object (SO_D)[115] to the Personalisation Agent.[116]

268 **Application Note 51 (taken from [7]):** 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

269	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

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

	FMT_SMR.1/PACE
FMT_MTD.1.1/AAPK	The TSF shall restrict the ability to create, load[117] the Active Authentication Private Key[118] to the Manufacturer and the Personalisation Agent.[119]

270 **Application Note 53 (of 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 [18])

271 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.[120]

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

1. the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,

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

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

273 **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.**

274 **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.**

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

275 **Application Note 52 (taken from [18]):** 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.

6.1.7 Class FPT Protection of the Security Functions

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

6.1.7.1 TOE Emanation (FPT_EMS)

FPT_EMS.1 TOE Emanation (taken from [18])

277 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit information about IC power consumption and command execution time[121] in excess of non useful information[122] 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. Personalisation Agent Key(s)[123]
5. Chip Authentication Private Key
6. Active Authentication Private Key[124] and
7. none.[125]

[121] [assignment: *types of emissions*]
[122] [assignment: *specified limits*]
[123] [assignment: *list of types of TSF data*],
[124] [assignment: *type of users*]
[125] [assignment: *list of types of user data*]

278 FPT_EMS.1.2 The TSF shall ensure any users[126] are unable to use the following interface smart card circuit contacts[127] 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. Personalisation Agent Key(s)
5. Chip Authentication Private Key(s)
6. Active Authentication Private Key[128] and
7. none.[129]

279 **Application note 54 (taken from [7]):** 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, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

6.1.7.2 Fail secure (FPT_FLS)

FPT_FLS.1 Failure with preservation of secure state (taken from [7])

280 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,[130]

6.1.7.3 TSF self test (FPT_TST)

FPT_TST.1 TSF testing (taken from [7])

281 Hierarchical to: No other components.

Dependencies: No dependencies.

[126] [assignment: *type of users*]
[127] [assignment: type of connection]
[128] [assignment: *list of types of TSF data*]
[129] [assignment: *list of types of user data*]
[130] [assignment: *list of types of failures in the TSF*]

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition[131] reset of the TOE[132] to demonstrate the correct operation of the TSF.[133]

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.[134]

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.[135]

6.1.7.4 TSF physical protection (FPT_PHP)

FPT_PHP.3 Resistance to physical attack (taken from [7])

282 Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[136] to the TSF[137] by responding automatically such that the SFRs are always enforced.

283 **Application Note 55 (taken from [7]):** 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.

6.2 Security Assurance Requirements for the TOE

284 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.

285 **Application note 56 (taken from [18]):** The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as

[131] [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*]

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

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

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

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

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

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

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

286 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.

287 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/ST 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 [5] 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).

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

289 The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Active Authentication Mechanism [6] 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/RSA_EMRTD.

6.3.2 Dependency Rationale

290 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.

291 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

292 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

293 This security target claims strict conformance to the Protection Profiles given in section 2.2. Therefore this security target includes the analysis of the internal consistency of the Security Requirements of the Protection Profiles without repeating these here.

294 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.

295 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.

296 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

297 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

298 The TOE provides access control mechanisms that allow the maintenance of different users (Manufacturer, Personalisation Agent, Terminal, PACE authenticated BIS-PACE, Country Verifying Certification Authority,Document Verifier, Domestic Extended Inspection System, Foreign Extended Inspection System).

299 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.

300 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 the Document Basic Access Keys.
- 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.

301 The access control mechanisms ensure that only the Country Verifying Certification Authority has the ability to update the CVCA Public Key and the CVCA Certificate. CVCA Public Key CVCA Certificates attributes are updated by the applet. The key is stored by the Platform, attributes are stored by the Applet.

302 The access control mechanisms ensure that only authenticated Extended Inspection System with the 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.

In these cases the TOE uses EAC, 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.

303 The access control mechanisms ensure that nobody is allowed to read the Document Basic Access Keys, the Chip Authentication Private Key, the Personalisation Agent Keys, and the Active Authentication Private Key.

304 A terminal authenticated as CVCA or as DV is explicitly denied to read data in the EF.DG3 and EF.DG4.

305 Any terminal is explicitly denied to modify any of the EF.DG1 to EF.DG16 of the logical travel document.

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

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

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

309 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, the authentication control is provided by TSF_Authenticate.

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.

FDP_UCT.1/TRM: It is a requirement about access control for details see the SFR), the access control is provided by TSF_AccessControl.

FDP_UIT.1/TRM: It is a requirement about access control for details see the SFR), the access control is provided by TSF_AccessControl

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_UAU.4/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.5/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.6/EAC: 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.6/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.

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.

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

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.

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.

FMT_MTD.1/KEY_READ: This requirement is about restriction of the ability to read out certain passwords and keys. It is realized by TSF.AccessControl, the key management is provided by TSF_Cryptokey_MRTD.

FMT_MTD.1/PA: This requirement is about restriction of the ability to 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.

FMT_MTD.3: This requirement is ensures that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol Version 1 and the Access Control. This is realized by TSF_Accesscontrol.

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. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. 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. It is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate. The control before the operational phase is provided by 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.

FTP_ITC.1/PACE: The requirement is about a separate communication channel which is provided by TSF_Authenticate.

7.1.2 TSF_Authenticate

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

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

312 The Platform contains a deterministic random number generator rated K4 (high) according to AIS20 [20] that provides random numbers used for the authentication. The seed for the deterministic random number generator is provided by the P2 (high) true random number generator of the underlying Platform.

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

- Chip Authentication Protocol
- Active Authentication Mechanism

314 The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol
- Symmetric Authentication Mechanism based on AES

315 Personalisation Agent authenticates himself to the TOE by use of the Personalisation Agent Keys with the following cryptographic mechanisms:

- Symmetric Authentication Mechanism

316 After completion of the PACE Protocol or the Chip Authentication Protocol, the TOE accepts commands with correct message authentication code only. These are calculated by the applet using security functions of the Platform. These commands must have been sent via secure messaging using the key previously agreed with the terminal during the last authentication.

317 The TOE accepts terminal authentication attempts by means of the Terminal Authentication Protocol only via secure messaging that was established by the preceding Chip Authentication Protocol.

318 The TOE verifies each command received after successful completion of the Chip Authentication Protocol as having been sent by the GIS.

319 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.

320 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, the authentication control is provided by TSF_Authenticate.

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/ST: The SFR is about Chip Authentication Mechanism which is provided by TSF_Authenticate.

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 what can be accessed before and after it. It is realized by TSF_Authenticate and TSF_AccessControl.

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_AccessControl.

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_AccessControl.

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_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/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_CryptoKey_MRTD.

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

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.

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.

FMT_MTD.1/PA: This requirement is about restriction of the ability to 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.

FMT_SMR.1/PACE: Requires the maintenance of security roles, this is realized by TSF.AccessControl, the authentication control is provided by TSF.Authenticate.

FIA_API.1/AA: The requirement is about the Active Authentication, which is provided by TSF_Authenticate.

7.1.3 TSF_SecureManagement_MRTD

321 The life cycle of TOE is split up in several phases. 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.

322 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.

323 The TSF provides functionality for the following SFRs:

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

FMT_LIM.2: The requirement is about restricting availibilities after TOE delivery, which is provided by TSF_SecureManagement_MRTD.

7.1.4 TSF_CryptoKey_MRTD

324 The TOE supports onboard generation of cryptographic keys based on the ECDH compliant [13] as well as generation of RSA and ECDSA key pairs. The Key generation is provided by the Platform.

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

326 The TOE supports overwriting the cryptographic keys with zero values as follows:

- the PACE Session Keys after detection of an error in a received command by verification of the MAC, and after successful run of the Chip Authentication Protocol, (In this case PACE session keys are overwritten by session keys created by CA)
- the Chip Authentication Session Keys after detection of an error in a received command by verification of the MAC,
- any session keys before starting the communication with the terminal in a new power-on-session.

327 The TSF provides functionality for the following SFR::

FCS_CKM.1/AA_GEN: The SFR requires generation of cryptographic keys. It is realized by TSF_CryptoKey_MRTD, 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_MRTD, 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_MRTD, 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_MRTD, 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_MRTD.

FCS_COP.1/SIG_VER: Requires a use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

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_MRTD and also TSF_Platform.

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_CryptoKey_MRTD.

FMT_MTD.1/KEY_READ: This requirement is about restriction of the ability to read out certain passwords and keys. It is realized by TSF.AccessControl, the key management is provided by TSF_Cryptokey_MRTD.

7.1.5 TSF_AppletParameters_Sign

328 During the Applet life cycle phases after LOADED state the applet becomes the default Application and reaches SELECTABLE state. This is called the Initialization phase. During this phase the following steps are carryed out:

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

329 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 can not be finished by reaching the INITIALIZED state, and the Personalization phase can not be started without successful signature verification.

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

331 The TSF provides functionality for the following SFRs::

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

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

7.1.6 TSF_Platform

332 There are security functionalities based on the security functionalities of the certified cryptographic library and the certified IC platform. This TSF covers those functionalities.

333 The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation.

334 The TOE is resistant to physical tampering on the TSF. This is managed by the Platform. If the TOE detects with the above mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

335 The TOE demonstrates the correct operation of the TSF by among others verifying the integrity of the TSF and TSF data and verifying the absence of fault injections. In the case of inconsistencies in the calculation of the signature and fault injections during the operation of the TSF the TOE preserves a secure state. Both the Applet and the Platform manage this.

336 The TOE supports the calculation of block check values for data integrity checking. These block check values are stored with persistently stored assets of the TOE as well as temporarily stored hash values for data to be signed. Both CRC and HASH function are calculated by the Platform

337 The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

338 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_MRTD, 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_MRTD, 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_MRTD, 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_MRTD, and because it uses Platform functionalities, TSF_Platform.

FCS_COP.1/CA_ENC: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/CA_MAC: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/PACE_ENC: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/PACE_MAC: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/RSA_EMRTD: Requires use of operation which is provided by TSF_Platform.

FCS_COP.1/SIG_VER: Requires use of cryptographic operation. It is provided by TSF_CryptoKey_MRTD and TSF_Platform.

FCS_RND.1: Requires use of operation which is provided by TSF_Platform.

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_MRTD and also 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_AppletParameters_Sign and 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_AppletParameters_Sign and TSF_Platform.

7.2 Assurance Measures

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

340 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 Userguide documentation, the AdminGuide document and in the InitandConf documentation.
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.

Table 10 References of Assurance measures

7.3 Fulfilment of the SFRs

341 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_MRTD	TSF_Cryptokey_MRTD	TSF_Appletparameters_sign	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.4				X		
FCS_COP.1/CA_ENC						X
FCS_COP.1/CA_MAC						X
FCS_COP.1/PACE_ENC						X
FCS_COP.1/PACE_MAC						X
FCS_COP.1/RSA_EMRTD						X
FCS_COP.1/SIG_VER				X		X
FCS_RND.1						X
FDP_ACC.1/TRM	X	X				
FDP_ACF.1/TRM	X	X				
FDP_RIP.1				X		X
FDP_UCT.1/TRM	X					
FDP_UIT.1/TRM	X					
FIA_AFL.1/PACE	X	X				
FIA_API.1/ST		X				
FIA_API.1/AA		X				
FIA_UAU.1/PACE	X	X				
FIA_UAU.4/PACE	X	X				
FIA_UAU.5/PACE	X	X				
FIA_UAU.6/EAC	X	X				
FIA_UAU.6/PACE	X	X				
FIA_UID.1/PACE	X	X				
FMT_LIM.1			X			
FMT_LIM.2			X			

FMT_MTD.1/AAPK	X					
FMT_MTD.1/CAPK	X	X		X		
FMT_MTD.1/CVCA_INI	X	X				
FMT_MTD.1/CVCA_UPD	X	X				
FMT_MTD.1/DATE	X	X				
FMT_MTD.1/INI_DIS	X					X
FMT_MTD.1/INI_ENA	X					X
FMT_MTD.1/KEY_READ	X			X		
FMT_MTD.1/PA	X	X				
FMT_MTD.3	X					
FMT_SMF.1	X	X				
FMT_SMR.1/PACE	X	X				
FPT_EMS.1						X
FPT_FLS.1					X	X
FPT_PHP.3						X
FPT_TST.1					X	X
FTP_ITC.1/PACE	X					

Table 11: Mapping of SFRs to mechanisms of TOE

7.3.1 Correspondence of SFR and TOE mechanisms

342 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.

7.4 Rationale for PP Claims

343 This security target is conformant to the claimed PPs [7] and [18]. Additionally, the Active Authentication Mechanism, the key generation of the Chip Authentication and Active Authentication keys on the TOE are included in the TOE. This implies the below described augmentations.

344 Addition of new TOE Assumptions:

- A.Sec_Manufac

345 Addition of new TOE Objectives:

- OT.Active_Auth_Proof

346 Addition of new IT Environment Objectives:

- OE.Active_Auth_Key_Travel_Document
- OE.Sec_Manufac

347 Addition of new SFRs for the TOE:

- FCS_CKM.1/AA_GEN
- FCS_CKM.1/CA_GEN
- FIA_API.1/AA
- FMT_MTD.1/AAPK
- FCS_COP.1/RSA_EMRTD

348 Extension of existing SFRs for the TOE to include the Active Authentication private key:

- FMT_MTD.1/KEY_READ
- FPT_EMS.1

8 Glossary and Acronyms

349 For Glossary and Acronyms please refer to the corresponding section of [18]

9 Bibliography

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

[2] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

[3] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

[4] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[5] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012

[6] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Sixth Edition, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)

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

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

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

[10] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2007-09-004 , Version 3.1, Revision 3, July 2009

[11] ISO/IEC 11770-3: Information technology — Security techniques — Key management -- Part 3: Mechanisms using asymmetric techniques, 2008

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

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical

Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009

[14] ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008

[15] ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11

[16] NSCIB-CC-13-13-37760-CR NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Certification Report by TÜV Rheinland Nederland B.V. , 2013 August 12th.

[17] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2010

[18] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012, version 1.3.0, 20th January 2012

[19] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Revision 1, 2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 02.12.1999

[21] NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Security Target Rev. 01.02 — 2nd August 2013 NSCIB-CC-13-37760

[21a] NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 Security Target Lite, Rev. 00.02 — 2nd August 2013, NSCIB-CC-13-37760

[22] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

[23] IDentity Applet Administrator's Guide Version 3.2.07

[24] IDentity Applet User's Guide Version 3.2.18

[25] IDentity Applet Initialization and configuration Version 3.2.19

[26] CCDB-2012-04-001 Composite product evaluation for Smart Cards and similar devices April 2012 Version 1.2 Mandatory Technical document

[27] ETR for Composite Evaluation NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 EAL5+ 9 August 2013

[28] GlobalPlatform Card Specification Version 2.2.1 Public Release January 2011

[29] Runtime Environment Specification Java Card(tm) Platform, Version 3.0.1 Classic Edition, May 2009, Sun Microsystems, Inc

[30] Technical Guideline TR-03110-2 Advanced Security Mechanisms forMachine Readable Travel Documents and eIDAS Token – Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS) Version 2.20 3. February 2015

[31] Technical Guideline TR-03110-4 Advanced Security Mechanisms forMachine Readable Travel Documents and eIDAS Token – Part 4 – Applications and Document Profiles Version 2.20 3. February 2015