STARCOS 3.5 ID SAC+EAC+AA C1

Security Target Lite

Version 2.2

R&D

Author	stut
Status	Final
Rating	Public
Edition	10.07.2012

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
D-81607 München

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
D-81607 München

Contents

1 ST Introduction

1.1 ST Reference

Title: Security Target STARCOS 3.5 ID SAC+EAC+AA C1

Reference: GDM_STA35_SAC_EAC_AA_C1_ASE

Version 2.2/10.07.2012

Origin: Giesecke & Devrient GmbH

Author: Henning Daum

CC Version: 3.1 (Revision 3)

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

TOE: STARCOS 3.5 ID SAC+EAC+AA C1

TOE documentation:

Preparative procedures STARCOS 3.5 ID SAC+EAC+AA C1

Operational user guidance STARCOS 3.5 ID SAC+EAC+AA C1

HW-Part of TOE: Infineon M7820 (Certificate: BSI-DSZ-CC-0813-2012)[43]. This TOE was evaluated against Common Criteria Version 3.1.

1.2 TOE Overview

This security target defines the security objectives and requirements for the contactless chip of machine readable travel documents based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). It addresses the advanced security methods Password Authenticated Connection Establishment and Extended Access Control, Chip Authentication and Active Authentication as defined in BSI TR-03110 [5], ICAO TR-SAC [4] and ICAO Doc 9303 [6].

If a product is using the BAC-established communication channel (see TOE documentation) it will not be conformant to the claimed PPs [37], [7] 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 current PPs [37], [7].

In the following chapters STARCOS 3.5 ID SAC+EAC+AA C1 stands for the Target of Evaluation (TOE). The related product is the STARCOS 3.5 ID SAC+EAC+AA C1 Card.

STARCOS 3.5 ID SAC+EAC+AA C1 consist of the related software in combination with the underlying hardware ('Composite Evaluation') including the STARCOS35PETABLES [45] and the GMA Verifier[1] [46] including its configuration file.

The TOE software is the STARCOS 3.5 ID operating system and the ePass application. The TOE hardware is the secure Infineon M7820 A11 certified according to CC EAL5+ with the following configurations according to [43]:

[1] The GMA Verifier is not part of the TOE delivery. It is solely used by the MRTD Manufacturer for the correct installation of the TOE and therefore of no use for the Personalisation Agent.

- NVM: 36 kByte up to 128 kByte
- ROM: 280 kByte
- XRAM: 8 kByte
- SCP: Accessible
- Crypto2304T: Accessible
- Interfaces: ISO/IEC 14443

The sales names of the TOE hardware platform [43] and the corresponding TOE names of STARCOS 3.5 ID SAC+EAC+AA C1 are listed below:

Sales name of M7820 A11 [43]	**TOE name of STARCOS 3.5 ID SAC+EAC+AA C1**
SLE78CLX360P	STARCOS 3.5 ID SAC+EAC+AA C1/360
SLE78CLX800P	STARCOS 3.5 ID SAC+EAC+AA C1/800
SLE78CLX1280P	STARCOS 3.5 ID SAC+EAC+AA C1/1280

In addition to the BSI-PP-0056-V2 [37] the STARCOS 3.5 ID SAC+EAC+AA C1 supports the Active Authentication mechanism as defined in [6].

The assurance level for the TOE is CC EAL4 augmented.

1.3 TOE Definition

The Target of Evaluation (TOE) addressed by this security target is an electronic travel document representing a contactless 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 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 (PACE PP), BSI-CC-PP-0068-V2 [7].

The TOE comprises of at least

- the circuitry of the travel document’s chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the ePassport application and
- the associated guidance documentation.

The TOE operating system does not include other applications than the ePassport application.

1.4 TOE Usage and Security Features for Operational Use

A State or Organisation issues travel documents to be used by the holder for international travel. The traveller presents a travel document to the inspection system to prove his or her identity. The travel document in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the travel document's chip according to LDS in case of contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation.

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.

(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 contactless integrated circuit. It presents 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 both2

  (d) the other data according to LDS (EF.DG5 to EF.DG16) and

  (e) the Document Security Object (SOD).

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.

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.

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.

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

[2] These biometric reference data are optional according to [6]. This ST assumes that the issuing State or Organisation uses this option and protects these data by means of extended access control.

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.

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].

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).

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.

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].

The security target requires the TOE to implement the Extended Access Control as defined in [5] and additionally the Active Authentication described in [6]. 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 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.

1.5 TOE life-cycle

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.)

Phase 1 “Development”

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

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the ePassport application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the ePassport application and the guidance documentation is securely delivered to the travel document manufacturer.

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). 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.

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

(Step4 optional) The travel document manufacturer combines the IC with hardware for the contactless interface in the travel document unless the travel document consists of the card only.

(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, (ii) creates the ePassport application, and (iii) equips travel document’s chips with pre-personalization Data.

Application Note 1 (taken from [37]): Creation of the application implies:

- For file based operating systems: the creation of MF and ICAO.DF
- For JavaCard operating systems: the Applet instantiation.

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.

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 holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the personalization of the visual readable data onto the physical part of the 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.

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.

Application Note 2 (taken from [37]): The TSF data (data created by and for the TOE, that might affect the operation of the TOE; cf. [1] §92) comprise (but are not limited to) the Personalisation Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key.

Application Note 3 (taken from [37]): 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.

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 Organisation and can be used according to the security policy of the issuing State but they can never be modified.

Application Note 4 (taken from [37]): The intention of the ST is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Since specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organisation. In this case the national body of the issuing State or Organisation is responsible for these specific production steps.
Note that the personalisation process and its environment may depend on specific security needs of an issuing State or Organisation. 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.
Some production steps, e.g. Step 4 in Phase 2 may also take place in the Phase 3.

1.6 Non-TOE Hardware/Software/Firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the 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.

1.7 Sections Overview

Section 1 provides the introductory material for the Security Target.

Section 2 provides the conformance claims for the Security Target.

Section 3 provides a discussion of the security problems for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the operational environment and the security objective rational to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat.

Section 5 contains the extended component definitions.

Section 6 contains the security functional requirements and assurance requirements derived from the Common Criteria [1], Part 2 [2] and Part 3 [3], which must be satisfied and the security functional requirements rational. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Section 7 contains the TOE Summary Specification.

Section 8 provides information on used acronyms and glossary and the used references.

2 Conformance Claim

2.1 CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [10]

has to be taken into account.

2.2 PP Claim

This ST claims strict conformance to the following Common Criteria Protection Profiles:

- Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 [37]
- Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011 [7]

2.3 Package Claim

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

3 Security Problem Definition

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.

The Assumptions included from the Protection Profiles are:

- A.Auth_PKI from [37]
- A.Insp_Sys from [37]
- A.Passive_Auth from [7]

The Threats included from the Protection Profiles are:

- T.Read_Sensitive_Data from [37]
- T.Counterfeit from [37]
- T.Skimming from [7]
- T.Eavesdropping from [7]
- T.Tracing from [7]
- T.Abuse-Func from [7]
- T.Information_Leakage from [7]
- T.Phys-Tamper from [7]
- T.Forgery from [7]
- T.Malfunction from [7]

The Organisational Security Policies included from the Protection Profiles are:

- P.Sensitive_Data from [37]
- P.Personalisation from [37]
- P.Pre-Operational from [7]
- P.Card_PKI from [7]
- P.Trustworthy_PKI from [7]
- P.Manufact from [7]
- P.Terminal from [7]

Application Note 5 (of the ST author): Active Authentication Mechansim 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

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.

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

- OT.Sens_Data_Conf from [37]
- OT.Chip_Auth_Proof from [37]
- 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.Identification from [7]
- OT.AC_Pers from [7]
- OT.Prot_Malfunction from [7]

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 authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Active Authentication as defined in [6]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

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

- OE.Auth_Key_Travel_Document from [37]
- OE.Authoriz_Sens_Data from [37]
- OE.Exam_Travel_Document from [37]
- OE.Prot_Logical_Travel_Document from [37]
- OE.Ext_Insp_Systems from [37]
- 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]

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

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.

Application Note 6 (of the ST author): Active Authentication Mechansim is an alternative to the Chip Authentication for identifying the TOE.

4.1 Security Objective Rationale

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.

In addtion 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".

5 Extended Components Definition

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

The Extended Components included from the Protection Profiles are:

- FIA_API from [37]
- FAU_SAS from [7]
- FCS_RND from [7]
- FMT_LIM from [7]
- FPT_EMS from [7]

6 Security Requirements

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.

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**.

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 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.

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 filled in by the ST author are denoted as double underlined text. 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*.

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.

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.

The following objects are defined in addtion 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}, KPu_{IAA}) 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 Private Key (KPr_{AA})	The Active Authentication Private Key (KPr_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.

6.1 Security Functional Requirements for the TOE

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 management (FCS_CKM)

FCS_CKM.1/DH_PACE Cryptographic key generation – Diffie-Hellman for PACE session keys (taken from [7])

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 avoid 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] [3,4] and specified cryptographic key sizes 112 bits[5], 128 bits, 192 bits and 256 bits[6,7] that meet the following: [4][8].

Application Note 7 (taken from [7]): The TOE generates a shared secret value with the terminal during 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 is used to derive session keys for message encryption and message authentication according to [4] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application Note 8 (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].

FCS_CKM.1/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys (taken from [37])

Hierarchical to: No other components.

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

[3] [selection: *Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [13]*]

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

[5] Cryptographic key size of 2-key Triple-DES session keys

[6] Cryptographic key sizes of AES session keys

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

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

ECDH protocol compliant to ISO 15946[9,10] and specified cryptographic key sizes 112 bits[11], 128 bits, 192 bits and 256 bits[12,13] that meet the following: based on an ECDH protocol compliant to [13][14].

Application Note 9 (taken from [37]): FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [5].

Application Note 10 (taken from [37]): 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]).

Application Note 11 (taken from [37]): 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 (cf. [5]). The TOE also implements additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol (cf. [5] for details).

FCS_CKM.1/CAPK Cryptographic key generation –Chip Authentication key pair

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.
FCS_CKM.4 Cryptographic key destruction: not fulfilled but justified.
Justification: The Chip Authentication key pair cannot be deleted or re-generated.

FCS_CKM.1.1/CAPK The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm G&D_ECDSAKeyGen[15] and specified cryptographic key sizes 224, 256, 320, 384, 512, 521 bits[16] that meet the following: curves brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according [39] and the curves secp256r1, secp384r1 and secp521r1 according [5], chapter A.2.1.1.[17].

[9] [selection: *based on the key Diffie-Hellman key derivation protocol compliant to PKCS#3, based on an ECDH protocol compliant to ISO 15946*]

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

[11] Cryptographic key size of 2-key Triple DES session keys

[12] Cryptographic key sizes of AES session keys

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

[14] [selection: *based on the Diffie-Hellman key derivation protocol compliant to [12] and [5], based on an ECDH protocol compliant to [13]*]

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

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

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

Application Note 12 (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 [37] (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/AAPK Cryptographic key generation –Active Authentication key pair

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 re-generated.

FCS_CKM.1.1/AAPK The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm G&D_RSAKeyGen[18] and specified cryptographic key sizes 2048 - 4096 bits[19] that meet the following: [6], chapter 8.2[20].

Application Note 13 (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.

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

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[21] that meets the following: none[22].

Application Note 14 (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

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

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

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

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

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

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.1)

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES/3DES (taken from [7])

Hierarchical to: No other components.

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

FCS_COP.1.1/PACE_ENC The TSF shall perform secure messaging – encryption and decryption[23] in accordance with a specified cryptographic algorithm AES and 3DES[24] in CBC mode[25] and cryptographic key sizes 112, 128, 192 and 256[26] [27] bit [28] that meet the following: compliant to [4][29].

Application Note 15 (taken from [7]): TOE implements the cryptographic primitives (i.e. Triple-DES and AES) for secure messaging with encryption of the transmitted data and encrypting the nonce in the first step of PACE. The 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/PACE_MAC Cryptographic operation – MAC (taken from [7])

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

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

[24] [selection: *AES, 3DES*]

[25] [assignment: *cryptographic algorithm*]

[26] For 3DES 112 bit cryptographic key size, for AES 128, 192 and 256 bit cryptographic key size

[27] [selection: *128, 192, 256*]

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

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

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[30] in accordance with a specified cryptographic algorithm CMAC and Retail-MAC[31] [32] [33] and cryptographic key sizes 112, 128, 192 and 256[34] [35] bit [36] that meet the following: compliant to [4][37].

Application Note 16 (of the ST author): The TOE to 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 PACE protocol according to FCS_CKM.1/DH_PACE.

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption (taken from [37])

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_ENC The TSF shall perform secure messaging – encryption and decryption[38] in accordance with a specified cryptographic algorithm AES and 3DES[39] and cryptographic key sizes 112, 128, 192 and 256 bit[40] [41] that meet the following: ICAO TR-SAC [4], chapter 4.6[42].

Application Note 17 (taken from [37]): 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 [37])

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

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

[31] For AES CMAC is used as MAC mechanism, for 3DES Retail-MAC is used as MAC mechanism

[32] [selection: *CMAC, Retail-MAC*]

[33] [assignment: *cryptographic algorithm*]

[34] For Retail-MAC 112 bit cryptographic key size, for CMAC 128, 192 and 256 bit cryptographic key size

[35] [selection: *112, 128, 192, 256*]

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

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

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

[39] [assignment: *cryptographic algorithm*]

[40] For 3DES 112 bit cryptographic key size, for AES 128, 192 and 256 bit cryptographic key size

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

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

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[43] in accordance with a specified cryptographic algorithm CMAC and Retail-MAC[44] and cryptographic key sizes 112, 128, 192 and 256 bits[45] [46] that meet the following: ICAO TR-SAC [4][47].

Application Note 18 (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.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document (taken from [37])

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[48] in accordance with a specified cryptographic algorithm ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[49] and cryptographic key sizes 192-521 bits[50,51] that meet the following: TR-03111 [13], chapter 4.1.2 using curves brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1 according [39] and curves secp256r1, secp384r1 and secp521r1 according [5], chapter A.2.1.1.[52].

Application Note 19 (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_MRTD Cryptographic operation – Signature generation

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

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

[44] [assignment: *cryptographic algorithm*]

[45] For Retail-MAC 112 bit cryptographic key size, for CMAC 128, 192 and 256 bit cryptographic key size

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

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

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

[49] [assignment: *cryptographic algorithm*]

[50] Bit length of curve

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

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

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_MRTD The TSF shall perform digital signature generation[53] in accordance with a specified cryptographic algorithm RSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512[54] and cryptographic key sizes: 1024 bits–4096 bits[55] that meet the following: scheme 1 of ISO/IEC 9796-2:2002 [32], Chapter 8[56,57].

Application Note 20a (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)

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])

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet K4 (high) according to AIS20 [41][58].

Application Note 21 (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

Application Note 22 (taken from [37]): The Table 1 provides an overview of the authentication mechanisms used.

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

[54] [assignment: *cryptographic algorithm*]

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

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

[57] According to [6], A4.2, the use of ISO/IEC 9796-2 Digital Signature scheme 1 is normative for the Active Authentication Mechanism.

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

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

Table 1 Overview on authentication SFRs

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

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

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.

FIA_AFL.1/PACE Authentication failure handling – PACE authentication using nonblocking authorisation data (taken from [7])

Hierarchical to: No other components.

Dependencies: UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

FIA_AFL.1.1/PACE The TSF shall detect when 15[59] [60] unsuccessful authentication attempts occurs related to authentication attempts using the PACE password as shared password[61].

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[62], the TSF shall delay each following authentication attempt until the next successful authentication attempt by approx. 4 seconds[63].

FIA_API.1 Authentication Proof of Identity (taken from [37])

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Note 23 (taken from [37]): The TOE implements the Chip Authentication Mechanism v.1 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_UID.1/PACE Timing of identification (taken from [37])

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/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 carry out the Chip Authentication Protocol Version 1 according to [5]
5. to carry out the Terminal Authentication Protocol Version 1 according to [5]
6. to carry out the Active Authentication Mechanism[66]

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

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

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

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

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

[64] [assignment: *authentication mechanism*]

[65] [assignment: *authorized user or role*]

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

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

FIA_UID.1.2/PACE The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 24 (taken from [37]): 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).

Application Note 25 (taken from [37]): 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).

Application Note 26 (taken from [37]): In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.
Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

FIA_UAU.1/PACE Timing of authentication (taken from [37])

Hierarchical to: No other components.

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

FIA_UAU.1.1/PACE The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [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[67]

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

FIA_UAU.1.2/PACE The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 27 (taken from [37]): 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 Terminal by the TOE (taken from [37])

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[68]
3. Terminal Authentication Protocol Version 1 according to [5][69]

Application Note 28 (of the ST author): The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

FIA_UAU.5/PACE Multiple authentication mechanisms (taken from [37])

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 MAC-ENC mode according to [4],
4. Symmetric Authentication Mechanism based on AES,[70]

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

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

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

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

5. Terminal Authentication Protocol Version 1 according to [5][71]

to support user authentication.

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[72].
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism Version 1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol Version 1 only if the terminal uses the public key presented during the Chip Authentication Protocol Version 1 and the secure messaging established by the Chip Authentication Protocol Version 1.[73]

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 ePassport application.

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

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. [74]

Application Note 30 (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-

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

[72] [selection: *the Authentication Mechanism with Personalization Agent Keys*]

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

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

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 – Re-authenticating of Terminal by the TOE (taken from [37])

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.[75]

Application Note 31 (taken from [37]): 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/AA Authentication Proof of Identity – travel document

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1/AA The TSF shall provide the Active Authentication Mechanism according to [6][76] to prove the identity of the TOE[77].

Application Note 32 (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 the claimed Protection Profiles.

6.1.3 Class FDP User Data Protection

FDP_ACC.1/TRM Subset access control (taken from [37])

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control: fulfilled by FDP_ACF.1/TRM

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

[76] [assignment: *authentication mechanism*]

[77] [assignment: *authorized user or role*]

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP[78] on terminals gaining access to the User Data and data in EF.SOD of the logical travel document[79].

FDP_ACF.1/TRM Security attribute based access control (taken from [37])

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: 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.

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[80] to objects based on the following:

1. Subjects:
   a. Terminal
   b. BIS-PACE
   c. Extended Inspection System,
2. Objects:
   a. data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document
   b. data in EF.DG3 of the logical travel document,
   c. data in EF.DG4 of the logical travel document,
   d. all TOE intrinsic secret cryptographic keys stored in the travel document[81],
3. Security attributes:
   a. PACE Authentication
   b. Terminal Authentication Version 1
   c. Authorisation of the Terminal[82]

FDP_ACF.1.2/TRM2 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.1.1/TRM according to [4] after a successful PACE authentication as required by FIA_UAU.1/PACE.[83]

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

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

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

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

[82] [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*]

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

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[84].

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following rules:

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.[85]

Application Note 33 (taken from [37]): 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.

Application Note 34 (taken from [37]): 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 Inspection Systems using PACE, see [4].

Application Note 35 (taken from [7]): Please note that the control on the user data transmitted between the TOE and the PACE terminal is addressed by FTP_ITC.1/PACE.

Application Note 36 (taken from [37]): 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.

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

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

FDP_RIP.1 Subset residual information protection (taken from [7])

Hierarchical to: No other components.

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[86] 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[87]),[88]

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD (taken from [7])

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[89] to be able to transmit and receive[90] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/TRM Data exchange integrity (taken from [7])

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[91] to be able to transmit and receive[92] user data in a manner protected from modification, deletion, insertion and replay[93] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[94] has occurred.

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

[87] according to [40], sec. 4.2.1, #3.b

[88] [assignment: *list of objects*]

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

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

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

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

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

6.1.4 Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE (taken from [7])

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. [95]

Application Note 37 (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.

Application Note 38 (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: 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.

Application Note 39 (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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[96] with the capability to store the Initialisation and Pre-Personalisation Data [97] in the audit records.

Application Note 40 (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

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

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

[96] [assignment: *authorised users*]

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

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

FMT_SMF.1 Specification of Management Functions (taken from [7])

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.[98]

FMT_SMR.1/PACE Security roles (taken from [37])

Hierarchical to: No other components.

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

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. Manufacturer,
2. Personalisation Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System
8. Foreign Extended Inspection System [99].

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

FMT_LIM.1 Limited capabilities (taken from [37])

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 does not allow,

1. User Data to be manipulated and disclosed,

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

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

2. TSF data to be disclosed or manipulated,
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,[100].

FMT_LIM.2 Limited availability (taken from [37])

Hierarchical to: No other components.

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

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow:

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,[101].

Application Note 41 (taken from [37]): The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.
Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

FMT_MTD.1/CVCA_INI Management of TSF data – Initialisation of CVCA Certificate and Current Date (taken from [37])

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

[100] [assignment: *Limited capability and availability policy*]

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[102] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date[103]

to the Personalisation Agent[104].

Application Note 42 (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 [37])

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 [105] the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate [106]

to Country Verifying Certification Authority [107].

Application Note 43 (taken from [37]): 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 [37])

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

[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*]

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify [108] the Current date [109] to

1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System [110].

Application Note 44 (taken from [37]): 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 [37])

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[111] the Chip Authentication Private Key[112] to the Manufacturer and the Personalisation Agent[113].

Application Note 45 (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/CAPK.

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

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 [114] the Initialisation Data and Pre-personalisation Data[115] to the Manufacturer. [116]

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

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

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

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

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[117] the Initialisation Data and the Pre-personalisation Data [118] to the Personalisation Agent. [119]

Application Note 46 (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'.

FMT_MTD.1/KEY_READ Management of TSF data –Key Read (taken from [37])

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[120] the

1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalization Agent Keys
4. **Active Authentication Private Key**[121]

to none[122].

Application Note 47 (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])

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

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

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

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

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

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

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 [123] the Document Security Object (SO_D)[124] to the Personalisation Agent. [125]

Application Note 48 (taken from [7]): By writing SO_D 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.3 Secure TSF data (taken from [37])

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[126].

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.**

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

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

Application Note 49 (taken from [37]): The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and

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

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

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

[126] [assignment: list of TSF data]

FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/AAPK The TSF shall restrict the ability to create, load[127] the Active Authentication Private Key[128] to the Manufacturer and the Personalisation Agent[129].

Application Note 50a (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.

6.1.7 Class FPT Protection of the Security Functions

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.

FPT_EMS.1 TOE Emanation (taken from [37])

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[130] in excess of non useful information[131] 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

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

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

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

[130] [assignment: *types of emissions*]

[131] [assignment: *specified limits*]

4. Personalisation Agent Key(s)
5. Chip Authentication Private Key
6. Active Authentication Private Key[132] and
7. none[133].

FPT_EMS.1.2 The TSF shall ensure any users[134] are unable to use the following interface smart card circuit contacts[135] to gain 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)
5. Chip Authentication Private Key
6. Active Authentication Private Key[136] and
7. none[137].

Application Note 51 (taken from [7]): The TOE prevents 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 can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 [14] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

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

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[138]

[132] [assignment: *list of types of TSF data*]

[133] [assignment: *list of types of user data*]

[134] [assignment: *type of users*]

[135] [assignment: *type of connection*]

[136] [assignment: *type of users*]

[137] [assignment: *list of types of user data*]

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the condition[139] Reset of the TOE[140] to demonstrate the correct operation of the TSF[141].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[142].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code[143].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [144] to the TSF [145] by responding automatically such that the SFRs are always enforced.

Application Note 52 (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

The 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 the following components:

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

Application Note 53 (taken from [37]): The TOE protects the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol (OE.Prot_Logical_Travel_Document). If the TOE is operated in non-certified mode using

[139] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*]

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

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

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

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

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

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

the BAC-established communication channel, the confidentiality of the standard data is 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

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.

The security objective **OT.Chip_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. This key can either be written to the TOE as defined by FMT_MTD.1/CAPK or created on the TOE itself as supported by FCS_CKM.1/CAPK. 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).
The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Active_Auth_Proof** "Proof of 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/AAPK. The Active Authentication Protocol requires additional TSF according to FCS_COP.1/RSA_MRTD.

6.3.2 Dependency Rationale

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

The dependency analysis has directly been made within the description of each SFR in section 6.1 above. All dependencies being expected by Common Criteria 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

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

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.

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.

The additions made to include the Active Authentication Mechansim 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.

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.

6.4 Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the Infineon derivates SLE78CLX360P, SLE78CLX800P, SLE78CLX1280P [43]. This statement is compliant to the requirements of [20].

6.4.1 Classification of Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as ‘relevant’ or ‘not relevant’ for the Composite-ST.

TOE Security Functionality	Relevant	Not relevant
SF_DPM: Device Phase Management	x	
SF_PS: Protection against Snooping	x	
SF_PMA: Protection against Modifying Attacks	x	
SF_PLA: Protection against Logical Attacks	x	
SF_CS: Cryptographic Support	x	

Table 2 Classification of Platform-TSFs

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

6.4.2 Matching statement

The TOE relies on fulfillment of the following implicit assumptions on the IC:

- Certified Infineon microcontroller derivates SLE78CLX360P, SLE78CLX800P, SLE78CLX1280P; the optional RSA2048/4096 v1.1.18, EC v1.01.018 and SHA-2 v1.1 libraries are not used by the composite TOE,
- True Random Number Generator (TRNG) with P2 classification according to AIS31 [42].
- Cryptographic support based on asymmetric and symmetric key algorithms (RSA, ECDSA, Triple-DES) with 1024-4096 bits (RSA modulus) and 192-521 bits (elliptic curve) asymmetric key length and 112 bits (2-key Triple-DES) symmetric cryptographic key length.

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

6.4.2.1 TOE Security Environment

For the TOE Security Environment of the Composite-ST please refer to chapter 3.

6.4.2.1.1 Threats and OSPs

None of the OSPs of the Composite-ST are applicable to the IC and therefore not mappable for the Platform-ST.

The augmented organisational security policy P.Add-Functions of the Platform-ST deals with additional specific security components like the AES encryption and decryption and can therefore be mapped to OT.Prot_Inf_Leak and OT.Prot_Phys-Tamper of the Composite-ST.

The following threats of this Composite-ST are directly related to IC functionality:

- T.Phys-Tamper
- T.Malfunction
- T.Abuse-Func
- T.Information_Leakage
- T.Forgery

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

- T.Leak-Inherent
- T.Phys_Probing
- T.Malfunction
- T.Phys_Manipulation
- T.Leak-Forced
- T.Abuse-Func
- T.RND
- T.Mem-Access

The following table shows the mapping of the threats.

Platform-ST		T.Leak-Inherent	T.Phys_Probing	T.Phys_Manipulation	T.Malfunction	T.Leak-Forced	T.Abuse-Func	T.RND	T.Mem-Access
Composite-ST	T.Phys_Tamper	x	x	x	x	x		x	
	T.Malfunction				x				
	T.Abuse-Func						x		x
	T.Information_Leakage	x	x	x	x	x	x		
	T.Forgery			x	x				

Table 3 Mapping of threats

T.Phys-Tamper matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.RND as physical TOE interfaces like emanations, probing, environmental stress and tampering are used to exploit vulnerabilities.

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

T.Information_Leakage matches to T.Leak-Inherent, T.Phys_Probing, T.Phys-Manipulation, T.Malfunction, T.Leak-Forced and T.Abuse-Func as physical TOE interfaces like emanations, probing, environmental stress and tampering could be used to exploit exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data.

T.Forgery matches to T.Phys_Manipulation and T.Malfunction 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 listed threats of the Platform-ST could be relevant.

6.4.2.1.2 Assumptions

The assumptions of this security target (see chapter 3) make no assumptions on the Platform.

The assumptions from the Platform-ST [43] are as follows:

Assumption	Classification of assumptions	Mapping to Security Objectives of this Composite-ST
A.Process-Sec-IC	not relevant	n/a
A.Plat-Appl	not relevant	n/a
A.Resp-Appl	relevant	OT.Data_Integrity, OT.Prot_Abuse-Func, OT.Prot_Phys-Tamper
A.Key-Function	relevant	OT.Prot_Inf_Leak

Table 4 Mapping of assumptions

There is no conflict between security environments of this Composite-ST and the Platform-ST [43].

6.4.2.2 Security objectives

For the TOE Security Environment of the Composite-ST please refer to chapter 4.

This Composite-ST has security objectives which are related to the Platform-ST. These are:

- OT.Prot_Abuse-Func
- OT.Prot_Inf_Leak
- OT.Prot_Phys-Tamper
- OT.Identification
- OT.Prot_Malfunction

The following platform objectives could be mapped to composite objectives:

- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Abuse-Func
- O.Leak-Forced
- O.Leak-Inherent
- O.Identification

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

Platform-ST		O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Abuse-Func	O.Leak-Forced	O.Leak-Inherent	O.Identification
Composite-ST	OT.Prot_Abuse-Func				x			
	OT.Prot_Inf_Leak					x	x	
	OT.Prot_Phys-Tamper	x	x	x				
	OT.Identification							x
	OT.Prot_Malfunction		x					

Table 5 Mapping of objectives

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

- O.Add-Functions cannot be mapped
- O.MEM_ACCESS is not relevant because the Composite-TOE does not use area based memory access control.
- None of the Security Objectives for the Environment are linked to the platform and are therefore not applicable to this mapping.

There is no conflict between security objectives of this Composite-ST and the Platform-ST [43].

6.4.2.3 Security requirements

6.4.2.3.1 Security Functional Requirements

This Composite-ST has the following platform-related SFRs:

- FAU_SAS.1
- FCS_COP.1/CA_ENC
- FCS_COP.1/CA_MAC
- FCS_COP.1/PACE_ENC
- FCS_COP.1/PACE_MAC
- FCS_COP.1/RSA_MRTD
- FCS_RND.1
- FMT_LIM.1
- FMT_LIM.2
- FPT_EMS.1
- FPT_FLS.1
- FPT_PHP.3
- FPT_TST.1

The following Platform-SFRs could be mapped to Composite-SFRs:

- FAU_SAS.1
- FCS_RNG.1
- FCS_COP.1/AES
- FCS_COP.1/DES
- FCS_COP.1/RSA
- FMT_LIM.1
- FMT_LIM.2
- FPT_FLS.1
- FPT_PHP.3
- FPT_TST.2
- FRU_FLT.2

They will be mapped as seen in the following table.

Platform-ST		FAU_SAS.1	FCS_RNG.1	FCS_COP.1/AES	FCS_COP.1/DES	FCS_COP.1/RSA	FMT_LIM.1	FMT_LIM.2	FPT_FLS.1	FPT_PHP.3	FPT_TST.2	FRU_FLT.2
Composite-ST	FAU_SAS.1	x										
	FCS_COP.1/CA_ENC			x	x							
	FCS_COP.1/CA_MAC			x	x							
	FCS_COP.1/PACE_ENC			x	x							
	FCS_COP.1/PACE_MAC			x	x							
	FCS_COP.1/RSA_MRTD					x						
	FCS_RND.1		x									
	FMT_LIM.1						x					
	FMT_LIM.2							x				
	FPT_EMS.1									x		
	FPT_FLS.1								x			
	FPT_PHP.3								x	x		x
	FPT_TST.1										x	

Table 6 Mapping of SFRs

FAU_SAS.1 of the Composite-ST matches to the equivalent SFR of the Platform-ST.

FCS_RND.1 of the Composite-ST matches FCS_RNG.1 of the Platform-ST when the hardware random number generator is used by the TOE.

FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC of the Composite-ST match FCS_COP.1/DES of the Platform-ST when the symmetric cryptography coprocessor is used by the TOE.

FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC of the Composite-ST match FCS_COP.1/AES of the Platform-ST when the symmetric cryptography coprocessor is used by the TOE.

FCS_COP.1/RSA_MRTD of the Composite-ST matches to FCS_COP.1/RSA of the Platform-ST when the asymmetric cryptography coprocessor is used by the TOE for digital signature generation.

FMT_LIM.1 and FMT_LIM.2 of the Composite-ST match to the equivalent SFR of the Platform-ST.

FPT_EMS.1 matches the FPT_PHP.3 of the Platform-ST.

FPT_FLS.1 matches to the equivalent SFR of the Platform-ST.

FPT_PHP.3 of the Composite-ST matches the robustness requirements of FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform-ST.

FPT_TST.1 matches the FPT_TST.2 of the Platform-ST.

The following Platform-SFRs are not mapped to Composite-SFRs:

- FCS_CKM.1/RSA, FCS_COP.1/ECDH and FCS_COP.1/ECSA because the TOE implements the cryptographic mechanisms and does not use the provided libraries of the platform TOE.
- FDP_ACC.1, because the composite TOE is always in system mode and therefore no MMU is necessary and because the composite TOE does not use the platform TOE special function registers.
- FDP_ACF.1, because the composite TOE does not use the platform TOE special function registers and the MMU.
- FMT_MSA.1, because the composite TOE is always in system mode and therefore no MMU and special function registers is necessary.
- FMT_MSA.3, because the composite TOE is always in system mode and therefore no MMU is necessary.
- FMT_SMF.1, because the TOE does not change the CPU mode.
- FDP_ITT.1, because it deals with the internal data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FPT_ITT.1, because it deals with the basic internal data protection of the platform TOE that does not by itself impact the composite TOE.
- FDP_IFC.1, because it deals with the data processing policy of the platform TOE that does not by itself impact the composite TOE.
- FDP_SDI.1 and FDP_SDI.2 are not applicable to the composite TOE. Protection against malfunctions is covered by the SFRs FPT_TST.1 and FPT_FLS.1 of the composite TOE.

6.4.2.3.2 Assurance requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1R3 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The Platform-ST requires EAL 5 according to Common Criteria V3.1 R3 augmented by: ALC_DVS.2 and AVA_VAN.5.

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

6.4.3 Analysis

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

7 TOE summary specification

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

7.1 TOE Security Functions

7.1.1 SF_AccessControl

The TOE provides access control mechanisms that allow among others the maintenance of different users (Manufacturer, Personalisation Agent, Country Verifying Certification Authority (CVCA), Document Verifier (DV), domestic Extended Inspection System, foreign Extended Inspection System).

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.

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.

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.

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 all other cases, reading any of the EF.DG3 to EF.DG4 of the logical travel document is explicitly denied.

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.

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

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

Only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol and the Access Control.

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.

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

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

7.1.2 SF_Authentication

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

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

The TOE contains a deterministic random number generator rated K4 (high) according to AIS20 [41] 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 IC.

The TOE supports user authentication by the following means:

- PACE Protocol
- Terminal Authentication Protocol
- Secure messaging in MAC-ENC mode
- Symmetric Authentication Mechanism based on AES

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

- Chip Authentication Protocol
- Active Authentication Mechanism

The TOE prevents reuse of authentication data related to:

- Terminal Authentication Protocol
- Symmetric Authentication Mechanism based on AES

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

- Symmetric Authentication Mechanism

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

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.

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

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

7.1.3 SF_AssetProtection

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.

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

7.1.4 SF_TSFProtection

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

The TOE is resistant to physical tampering on the TSF. 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.

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.

7.1.5 SF_KeyManagement

The TOE supports onboard generation of cryptographic keys based on the ECDH compliant [13] as well as generation of RSA and ECC key pairs.

A successfully authenticated Personalisation Agent is allowed to change the Personalisation Agent Keys.

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.

7.2 Assurance Measures

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

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 operational user guidance documentation and in the documentation for preparative procedures.
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 7 References of Assurance measures

7.3 Fulfilment of the SFRs

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

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement
FAU_SAS.1	x				
FCS_CKM.1/AAPK					x
FCS_CKM.1/CA					x
FCS_CKM.1/CAPK					x
FCS_CKM.1/DH_PACE					x
FCS_CKM.4					x
FCS_COP.1/CA_ENC		x		x	
FCS_COP.1/CA_MAC		x		x	
FCS_COP.1/PACE_ENC		x		x	
FCS_COP.1/PACE_MAC		x		x	
FCS_COP.1/RSA_MRTD		x		x	
FCS_COP.1/SIG_VER		x		x	
FCS_RND.1		x		x	

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement
FDP_ACC.1/TRM	x				
FDP_ACF.1/TRM	x				
FDP_RIP.1					x
FDP_UCT.1/TRM		x			
FDP_UIT.1/TRM		x			
FIA_AFL.1/PACE		x			
FIA_API.1		x			
FIA_API.1/AA		x			
FIA_UAU.1/PACE		x			
FIA_UAU.4/PACE		x			
FIA_UAU.5/PACE		x			
FIA_UAU.6/EAC		x			
FIA_UAU.6/PACE		x			
FIA_UID.1/PACE		x			
FMT_LIM.1	x		x		
FMT_LIM.2	x		x		
FMT_MTD.1/AAPK	x				
FMT_MTD.1/CAPK	x				
FMT_MTD.1/CVCA_INI	x				
FMT_MTD.1/CVCA_UPD	x				
FMT_MTD.1/DATE	x				
FMT_MTD.1/INI_DIS	x				
FMT_MTD.1/INI_ENA	x				
FMT_MTD.1/KEY_READ	x				
FMT_MTD.1/PA	x				
FMT_MTD.3	x				
FMT_SMF.1	x				
FMT_SMR.1/PACE	x				
FPT_EMS.1			x		
FPT_FLS.1				x	
FPT_PHP.3				x	

TOE SFR / Security Function	SF_AccessControl	SF_Authentication	SF_AssetProtection	SF_TSFProtection	SF_KeyManagement
FPT_TST.1				x	
FTP_ITC.1/PACE	x				

Table 8 Mapping of SFRs to mechanisms of TOE

7.3.1 Correspondence of SRF and TOE mechanisms

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

This security target is conformant to the claimed PPs [7] and [37]. Additionally, the Active Authentication Mechanism and 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.

Addition of new TOE Objectives:

- OT.Active_Auth_Proof

Addition of new IT Environment Objectives:

- OE.Active_Auth_Key_Travel_Document

Addition of new SFRs for the TOE:

- FCS_CKM.1/AAPK
- FCS_CKM.1/CAPK
- FIA_API.1/AA
- FMT_MTD.1/AAPK

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

For Glossary and Acronyms please refer to the corresponding section of [37].

9 Bibliography

The bibliography has been structured so that references 1-19 are the same as used in [37].

9.1 Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[10] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[20] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0, CCDB-007-09-001

9.2 ICAO

[6] International Civil Avation Organisation, ICAO Doc 9303 incl. supplemental, Machine Readable Travel Documents – Machine Readable Passports, 2006

[4] International Civil Avation Organisation, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[21] International Civil Avation Organisation Facilitation (FAL) Division, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

9.3 Cryptography

[22] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[23] ISO/IEC 15946-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002

[24] ISO/IEC 15946-2: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002

[25] ISO/IEC 15946-3: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[26] U.S. Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 25 October 1999

[27] NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, US Department of Commerce, October 1999

[28] Federal Information Processing Standards Publication FIPS PUB 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, June 2009

[29] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[30] ANSI X9.19, AMERICAN NATIONAL STANDARD, Financial Institution Retail Message Authentication, 1996

[31] ANSI X9.62-1999, AMERICAN NATIONAL STANDARD, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

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

[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

[33] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, May 2005

[34] Request for Comments: 4493, The AES-CMAC Algorithm, JH. Song et al. University of Washington, Category: Informational, June 2006

9.4 Protection Profiles

[35] Common Criteria Protection Profile PP conformant to Smartcard IC Platform, BSI-PP-0002-2001, version 1.0, July 2001

[36] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[9] Common Criteria Protection Profile Security IC Platform, BSI-PP-0035-2007, version 1.0, June 2007

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

[37] 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

[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, 2nd November 2011

9.5 Technical Guidelines and Directives

[40] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 1.11, 17.04.2009, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[5] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection establishment (PACE), and restricted Identification (RI), Version 2.05, 14.10.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

[42] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31; Bundesamt für Sicherheit in der Informationstechnik, Version 1, 25.09.2001

9.6 Other

[14] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organisation, security and commands for interchange, FDIS 2005, Amd 1:2008

[15] ISO 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 2008

[43] Security Target M7820 A11, Infineon Technologies AG, Version 1.5, 2012-05-07

[45] STARCOS 3.5 ID TABLES, Giesecke & Devrient

[46] Generic MRTD Application Verifier Tool for STARCOS 3.5 ID, Giesecke & Devrient