MOS

COMMON CRITERIA

SECURITY TARGET OF EPASSPORT APPLICATION ON MOS

VERSION 1.0.0

26 FEBRUARY 2019

CONFIDENTIALITY

LEVEL 1 - PUBLIC

MOS-CC-SECURITYTARGET-1V0V0

DOCUMENT IDENTIFICATION

DEPARTMENT	AUTHOR	CLASSIFICATION
R&D	Chew Hoong Wei	Level 1 - Public

APPROVALS

APPROVING PARTY	VERSION APPROVED	SIGNATURE	DATE
Chas Yap Managing Director	1.0.0		

REVIEWS

REVIEWING PARTY	VERSION REVIEWED	SIGNATURE	DATE
Poh Tze Siang Senior Software Engineer	1.0.0		

REVISION HISTORY

VERSION	DATE	AUTHOR	REMARKS
1.0.0	26 Feb 2019	CHW	Release version

1 Contents

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This Security Target defines the security objectives and requirements of the Multi-application Operating System (MOS) as implemented as contact and/or contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It covers the requisite authentication mechanisms:

- Supplemental Access Control (SAC), i.e. Password Authenticated Connection Establishment version 2 (PACE)
- Extended Access Control version 1 (EAC), including Chip Authentication (CA) and Terminal Authentication (TA)
- Active Authentication (AA)

This Security Target is based on Protection Profile *Common Criteria Protection Profile — Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP)*. This ST makes various refinements to the above-mentioned PP. They are all properly identified in the text typeset as indicated here. The original text of the PP is repeated as scarcely as possible in this document for reading convenience.

1.1 ST REFERENCE

Title	Security Target – ePassport Application on MOS
Sponsor	MCS Microsystems Sdn Bhd
CC Version	3.1 (Revision 5)
Assurance Level	EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
General Status	Release
Version Number	1.0.0
Date	26 February 2019
Keywords	ICAO, Machine Readable Travel Document, Extended Access Control, PACE, Supplemental Access Control (SAC)

1.2 TOE REFERENCE

Product Name	Multi-application Operating System (MOS)
TOE Name	ePassport Application on MOS
TOE Hardware	ST31G480 C01
TOE Version	1.0.0
Release Date	15 March 2019

1.3 TOE OVERVIEW

The MCS Multi-Application Operating System (MOS) is a secure and powerful chip operating system purpose designed for trusted ID applications, especially e-passport and possibly ISO-compliant driving license and national ID. Its key features are:

- File Manager based on the ISO/IEC 7816 standard
- GlobalPlatform Card Manager
- Early Lifecycle Manager
- Biometric match-on-chip (optional)

The TOE hardware is the STMicrolectronics C01 platform including optional cryptographic library NESLIB and derivative devices as detailed below:

Table 1: Configuration of derivative devices.

Features	Possible values
I/O mode	Contact only, Dual mode, Contactless only
NVM size	480 Kbytes
Nescrypt	Active
MIFARE support (Crypto1 + LPU)	Inactive
Capacitor	20pF, 68pF

The TOE hardware security target name is *ST31G480 C01 including optional cryptographic library Neslib, and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X Security Target for Composition* ([ST31G_ST]).

1.3.1 TOE TYPE DEFINITION

The Target of Evaluation (TOE) type addressed by this Security Target is the contact/contactless integrated circuit chip of an electronic travel document programmed according to ICAO *Doc 9303 Machine Readable Travel Documents* ([ICAO]) and additionally providing the Extended Access Control according to BSI *TR-03110* ([TR-03110]). The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to protection profile *BSI-CC-PP-0068-V2 Machine Readable Travel Documents using Standard Inspection Procedure with PACE (PACE PP)* ([PP-0068]).

The TOE comprises:

- the circuitry of the travel document's chip (ST31G480 integrated circuit (IC) revision C01.1),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software (cryptographic library Neslib 4.2.10),
- the IC Embedded Software (Multi-Application Operating System (MOS)),
- the epassport application and
- the associated guidance documentation (see ([MOS_UGD])).

1.3.2 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE

A State or Organization 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 ([ICAO]) for contactless or contact based machine reading. The authentication of the traveller is based on (i) the possession of a valid travel document personalized 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 organization ensures the authenticity of the data of genuine travel documents. The receiving state trusts a genuine travel document of an issuing State or Organization.

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

The issuing State or Organization 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 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, personalization procedures) ([ICAO]). These security measures 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 Organization 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 Encryption of sensitive biometrics as optional security measure and Password Authenticated Connection Establishment in the ICAO Doc 9303 ([ICAO]). 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 ([TR-03110]) as an alternative to the Active Authentication stated in ([ICAO]).

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless, this is not explicitly covered by this security target as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the travel document using BAC will not be conformant to the current security target; i.e. a product implementing the TOE may functionally use BAC, but, while performing BAC, they are acting outside of security policy defined by the current security target. Therefore, organisations being responsible for the operation of inspection systems shall be aware of this context.

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)* ([PP-0068]). Note that ([PP-0068]) considers high attack potential.

For the PACE protocol according to ([ICAO]), the following steps shall be performed:

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys K_{MAC} and K_{ENC} from the shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation, the terminal and the travel document's chip provide private communication (secure messaging) ([TR-03110]), ([ICAO]).

The security target requires the TOE to implement the Extended Access Control as defined in ([TR-03110]). 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 security target also requires the TOE to implement Active Authentication as defined in ([ICAO]). Keys for Chip authentication and Active Authentication can be loaded into the card (or optionally generated by the card). This operation takes place at personalization time.

Although the TOE is the ePassport Application, the product may also be used as an ISO driving license, compliant to ISO/IEC 18013 standard ([ISO_18013]) supporting EAC version 1 and Active Authentication, as both applications (travel document and ISO driving license) share the same protocols and data structure.

The table below indicates how terms and concepts present in the current document shall be read when considering the product as an ISO driving license:

Table 2: Terms corresponding to travel document and ISO driving license.

Travel Document	ISO Driving License
Travel document	ISO driving license
ICAO	ISO/IEC
ICAO Doc 9303	ISO/IEC 18013
DG3	DG7
DG4	DG8
DG15	DG13
MRZ	MRZ or SAI (Scanning area identifier)
Traveller	Cardholder

1.3.3 TOE LIFE-CYCLE

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to the ([PP-0084]), the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

Phase 1 "Development"

Step 1 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.

Step 2 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), 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"

Step 3 In a first step, the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the travel document's chip Embedded Software in the non-volatile non-programmable memory (ROM) and non-volatile programmable memory (NVM). 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 manufacturer to the travel document manufacturer.

If necessary, the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (NVM).

Step 4 (optional) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the card only.

Step 5 The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (NVM) if necessary, (ii) creates the ePassport application, and (iii) equips travel document's chips with pre-personalization Data.

Note 1: Creation of the application implies the creation of MF and ICAO.DF.

Phase 3 "Personalisation of the travel document"

Step 6 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.

Note 2: The TSF data (data created by and for the TOE, that might affect the operation of the TOE 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.

Note 3: 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 ([ICAO]). This approach allows but does not enforce the separation of these roles.

Phase 4 "Operational Use"

Step 7 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.

Note 4: The intention of the security target is to consider phase 1 and parts of phase 2 (i.e. Step 1 to Step 3) as part of the evaluation and therefore to define the TOE delivery according to CC after this phase. Specific production steps of phase 2 are of minor security relevance (e.g. booklet manufacturing and antenna integration). Note that the personalisation process and

its environment may depend on specific security needs of an issuing State or Organisation. This Security Target outlines 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.

The scope of evaluation of this Security Target is limited to phase 1 and part of phase 2 (i.e. Step 1 to Step 3) of the TOE life-cycle described above. Therefore, the list of relevant sites are as follows:

- STMicroelectronics development and production sites of the "ST31G480 C01" IC, see ([ST31G_ST]) Table 16.
- MCS Microsystems development site.

Other production sites for the rest of the TOE life-cycle shall be determined in future and shall be expected to have a secure environment.

1.3.4 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.

1.4 TOE DESCRIPTION

The TOE comprises:

- the circuitry of the travel document's chip (ST31G480 integrated circuit (IC) revision C01.1),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software (cryptographic library Neslib 4.2.10),
- the IC Embedded Software (Multi-Application Operating System (MOS)),
- the epassport application and
- the associated guidance documentation (see Table 3).

1.4.1 PHYSICAL SCOPE OF THE TOE

The physical scope of the TOE is presented below:

Table 3: Physical components of TOE.

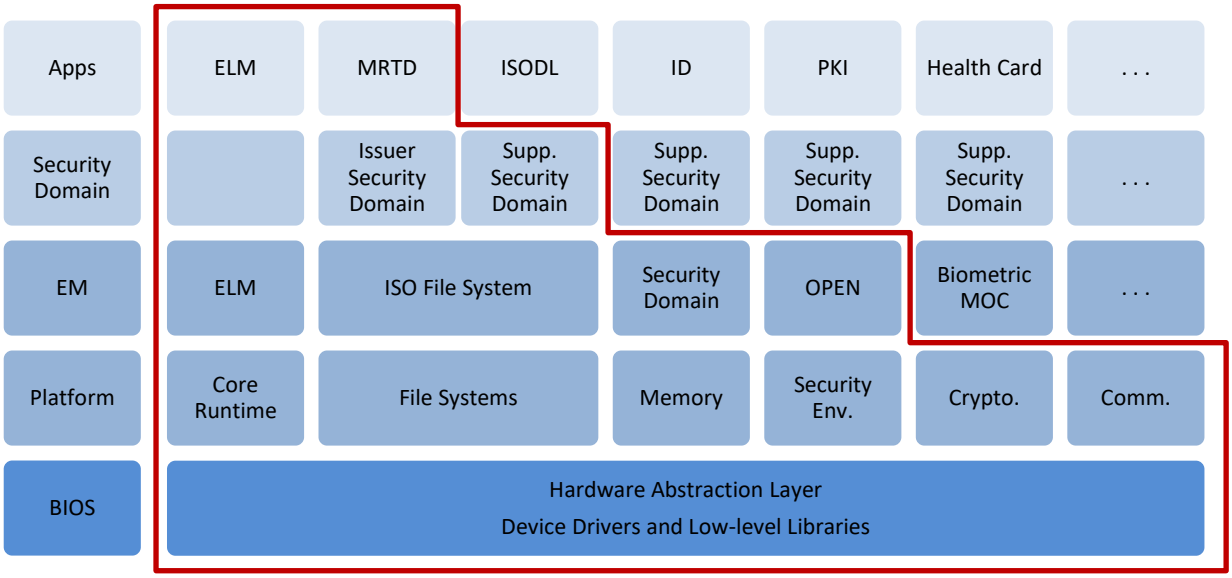
Item	Description	Format	Delivery Method	Delivered By
1	ST31G480 integrated circuit (IC) revision C01.1 ([ST31G_ST])	Wafer or Module	Courier delivery	STMicroelectronics
2	MOS Functional Specifications ([MOS_FSP])	PDF	Encrypted Email	MCS

3	MOS Early Lifecycle Manager Functional Specifications ([MOS_ELM])	PDF	Encrypted Email	MCS
4	MOS User Guidance ([MOS_UGD])	PDF	Encrypted Email	MCS
5	Pre-personalisation Agent Authentication Key	Hex	Encrypted Email	MCS

1.4.2 LOGICAL SCOPE OF THE TOE

The logical scope of the TOE is within the red outline as shown below:

Figure 1: Logical scope of TOE.



The TOE can be divided into four virtual layers:

- Basic input/output system (BIOS)
- Platform and executable module (EM)
- Security Domain, including Issuer Security Domain and Supplementary Security Domain
- Application

2 Conformance Claims

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-2017-04-001, Version 3.1, Revision 5, April 2017* ([CC_P1])
- *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* ([CC_P2])
- *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017* ([CC_P3])

as follows

  - Part 2 extended,
  - Part 3 conformant.

The

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

has to be taken into account.

2.2 PP CLAIM

This security target claims strict conformance to

- *Protection Profile – Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02* ([PP-0056]),

which in turn claims strict conformance to

- *Protection Profile – Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2* ([PP-0068]).

This security target is of a composed TOE and the security target of the following component is referred:

- *ST31G480 C01 including optional cryptographic library Neslib, and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X Security Target for Composition* ([ST31G_ST])

2.3 PP ADDITIONS

Active Authentication based on ICAO PKI v1.1 [ICAO_PKI] has been added. This implies the following augmentations:

- Extension of existing Assumptions for the TOE:
  - A.Insp_Sys: Inclusion of Active Authentication
- Addition of a new security objective for the TOE:
  - OT.Active_Auth_Proof
- Addition of a new security objective for the TOE environment:
  - OE.Active_Auth_Key_Travel_Document
- Addition of new SFRs for the TOE
  - FCS_COP.1/AA AA signature creation by travel document
  - FIA_API.1/AA Authentication Proof of Identity
  - FDP_ITC.1 Import of user data without security attributes
  - FMT_MTD.1/AAPK Management of TSF data – Active Authentication Private Key

2.4 PACKAGE CLAIM

This security target conforms to assurance package EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 defined in CC Part 3 ([CC_P3]).

2.5 CONFORMANCE CLAIM RATIONALE

The TOE type of this security target is "the contact/contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and additionally providing the Extended Access Control and Supplemental Access Control according to the *ICAO Doc 9303* ([ICAO]) and *BSI TR-03110* ([TR-03110])", compatible with the expected TOE type described in the PP.

This security target does not require a conformance claim rationale. ([PP-0056]) requires strict conformance of any ST claiming conformance to it.

3 Security Problem Definition

3.1 INTRODUCTION

Assets

The primary assets to be protected by the TOE as defined in section 3.1 from the claimed EAC PP ([PP-0056]) are listed in Table 4.

Table 4: Primary assets.

Object No.	Asset
1	User data stored on the TOE, including sensitive biometric reference data (EF.DG3, EF.DG4)
2	User data transferred between the TOE and the service provider connected (i.e. an authority represented by Basic Inspection System with PACE)
3	Travel document tracing data

The secondary assets to be protected by the TOE as defined in section 3.1 from the claimed EAC PP ([PP-0056]) are listed in Table 5.

Table 5: Secondary assets.

Object No.	Asset
4	Accessibility to the TOE functions and data only for authorized subjects
5	Genuineness of the TOE
6	TOE internal secret cryptographic keys
7	TOE internal non-secret cryptographic material
8	Travel document communication establishment authorisation data

The primary and secondary assets are defined in EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

Note 5: Due to interoperability reasons the ICAO *Doc 9303* ([ICAO]) requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC. Note that the BAC mechanism cannot resist attacks with high attack potential. If supported, it is therefore recommended to used PACE instead of BAC. If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks.

A sensitive asset to be protected by the TOE as defined in section 3.1 from the claimed EAC PP ([PP-0056]) is:

- Authenticity of the travel document's chip

Subjects and external entities

This security target considers the following subjects and external as defined in section 3.1 from the claimed EAC PP ([PP-0056]):

1. Country Verifying Certification Authority
2. Document Verifier
3. Terminal
4. Inspection system (IS), i.e. Extended Inspection System (EIS)
5. Attacker
6. Manufacturer
7. Personalisation Agent
8. Basic Inspection System with PACE (BIS-PACE)
9. Document Signer (DS)
10. Country Signing Certification Authority (CSCA)
11. Travel document holder
12. Travel document presenter (traveler)

The above subjects and external entities are defined in EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

3.2 THREATS

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

The threats are defined in section 3.3 of the EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

Table 6: Threats.

Label	Name	Reference
T.Read_Sensitive_Data	Read the sensitive biometric reference data	EAC PP ([PP-0056])
T.Counterfeit	Counterfeit of travel document chip data	EAC PP ([PP-0056])
T.Skimming	Skimming travel document / Capturing Card-Terminal Communication	PACE PP ([PP-0068])
T.Eavesdropping	Eavesdropping on the communication between the TOE and the PACE terminal	PACE PP ([PP-0068])
T.Tracing	Tracing travel document	PACE PP ([PP-0068])
T.Abuse-Func	Abuse of functionality	PACE PP ([PP-0068])
T.Information_Leakage	Information leakage from travel document	PACE PP ([PP-0068])
T.Phys-Tamper	Physical tampering	PACE PP ([PP-0068])
T.Forgery	Forgery of data	PACE PP ([PP-0068])
T.Malfunction	Malfunction due to environmental stress	PACE PP ([PP-0068])

Note 6: T.Forgery from the PACE PP ([PP-0068]) shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

3.3 ORGANISATIONAL SECURITY POLICIES

The TOE shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations (see CC part 1, sec. 3.2).

The OSPs are defined in section 3.4 of the EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

Table 7: Organisational security policies.

Label	Name	Reference
P.Sensitive_Data	Privacy of sensitive biometric reference data	EAC PP ([PP-0056])
P.Personalisation	Personalisation of the travel document by issuing State or Organisation only	EAC PP ([PP-0056])
P.Pre-Operational	Pre-operational handling of the travel document	PACE PP ([PP-0068])
P.Card_PKI	PKI for Passive Authentication (issuing branch)	PACE PP ([PP-0068])
P.Trustworthy_PKI	Trustworthiness of PKI	PACE PP ([PP-0068])
P.Manufact	Manufacturing of the travel document's chip	PACE PP ([PP-0068])
P.Terminal	Abilities and trustworthiness of terminals	PACE PP ([PP-0068])

3.4 ASSUMPTIONS

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

A.Insp_Sys Inspection Systems for global interoperability

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE ([ICAO]) and/or BAC ([PP-0055]). BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. Optionally, all the Inspection Systems can implement Active Authentication.

Justification:

The assumption A.Insp_Sys does not confine the security objectives of the ([PP-0056]) as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the Active Authentication functionality of the TOE.

This security target makes the assumptions A.Auth_PKI and A.Passive_Auth as defined in section 3.2 of the EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

Table 8: Assumptions.

Label	Name	Reference
A.Auth_PKI	PKI for Inspection Systems	EAC PP ([PP-0056])
A.Passive_Auth	PKI for Passive Authentication	PACE PP ([PP-0068])

4 Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organisational security policies to be met by the TOE.

Table 9: Security objectives of the TOE.

Label	Name	Reference
OT.Sens_Data_Conf	Confidentiality of sensitive biometric reference data	EAC PP ([PP-0056])
OT.Chip_Auth_Proof	Proof of the travel document's chip authenticity	EAC PP ([PP-0056])
OT.Data_Integrity	Integrity of Data	PACE PP ([PP-0068])
OT.Data_Authenticity	Authenticity of Data	PACE PP ([PP-0068])
OT.Data_Confidentiality	Confidentiality of Data	PACE PP ([PP-0068])
OT.Tracing	Tracing travel document	PACE PP ([PP-0068])
OT.Prot_Abuse-Func	Protection against Abuse of Functionality	PACE PP ([PP-0068])
OT.Prot_Inf_Leak	Protection against Information Leakage	PACE PP ([PP-0068])
OT.Prot_Phys-Tamper	Protection against Physical Tampering	PACE PP ([PP-0068])
OT.Prot_Malfunction	Protection against Malfunctions	PACE PP ([PP-0068])
OT.Identification	Identification of the TOE	PACE PP ([PP-0068])
OT.AC_Pers	Access Control for Personalisation of logical MRTD	PACE PP ([PP-0068])

The security objectives listed above are defined in section 4.1 of the EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

This security target adds the following security objective for the TOE.

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 Organization by means of the Active Authentication as defined in ([ICAO]). The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.
>
> **Note 7:** The OT.Active_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the

authentication attempt of travel document's chip i.e. a certificate for the Active Authentication Public Key that matches the Active Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Active Authentication Public Key (EF.DG15) in the LDS defined in ([ICAO]) and (ii) the hash value of DG15 in the Document Security Object signed by the Document Signer.

TOE security objectives OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing, OT.Prot_Abuse-Func, OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, OT.Prot_Malfunction and OT.Active_Auth_Proof address the protection provided by the TOE independent of TOE environment.

TOE security objectives OT.Identification and OT.AC_Pers address the aspects of identified threats to be countered involving TOE's environment.

4.2 SECURITY OBJECTIVE FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the TOE environment listed in Table 10, Table 11 and Table 12 are defined in section 4.2 of the EAC PP ([PP-0056]) and PACE PP ([PP-0068]). Due to identical definitions and names, they are not repeated here.

Issuing State or Organisation

The issuing State or Organisation will implement the following security objectives for the TOE environment.

Table 10: Security objectives of the Issuing State or Organisation.

Label	Name	Reference
OE.Auth_Key_Travel_Document	Travel document Authentication Key	EAC PP ([PP-0056])
OE.Authoriz_Sens_Data	Authorization for Use of Sensitive Biometric Reference Data	EAC PP ([PP-0056])
OE.Legislative_Compliance	Issuing of the travel document	PACE PP ([PP-0068])
OE.Passive_Auth_Sign	Authentication of travel document by Signature	PACE PP ([PP-0068])
OE.Personalisation	Personalisation of travel document	PACE PP ([PP-0068])

This security target adds the following security objective for the TOE environment.

OE.Active_Auth_Key_Travel_Document (Travel document Active Authentication Key)

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

Justification: This security objective for the operational environment is needed additionally to those from ([PP-0056]) in order to counter the Threat T.Counterfeit as it specifies the pre-

requisite for the Active Authentication which is one of the additional features of the TOE described in this security target and not in ([PP-0056]).

Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives for the TOE environment.

Table 11: Security objectives of the Receiving State or Organisation.

Label	Name	Reference
OE.Prot_Logical_Travel_Document	Protection of data from the logical travel document	EAC PP ([PP-0056])
OE.Ext_Insp_Systems	Authorization of Extended Inspection Systems	EAC PP ([PP-0056])
OE.Terminal	Terminal operating	PACE PP ([PP-0068])

This security target extends the following security objective for the TOE environment defined in ([PP-0056]).

OE.Exam_Travel_Document Examination of the physical part of the travel document

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

Justification: This security objective for the operational environment is needed additionally to those from ([PP-0068]) in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1, or optionally Active Authentication. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in ([PP-0068]) and therefore also counters T.Forgery and A.Passive_Auth from ([PP-0068]). This is done because a new type of Inspection System is introduced in ([PP-0056]) as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

Travel document holder Obligations

The travel document holder will implement the following security objectives for the TOE environment.

Table 12: Security objective of travel document holder.

Label	Name	Reference
OE.Travel_Document_Holder	Travel document holder Obligations	PACE PP ([PP-0068])

4.3 SECURITY OBJECTIVE RATIONALE

The following table provides an overview for security objectives coverage.

Table 13: Security objective rationale.

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

Detailed justifications required for suitability of the security objectives to cope with the security problem definition are given in section 4.3 of ([PP-0056]) and ([PP-0068]), with the following changes:

- Replace EAC PP ([PP-0056]) lines 594 to 603 with:

  The threat **T.Counterfeit** "Counterfeit of travel document chip data" addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip's identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" or **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 Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** "Travel document Authentication Key". 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". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 or Active Authentication to verify the authenticity of the travel document's chip.

- Replace EAC PP ([PP-0056]) lines 611 to 620 with:

  The examination of the travel document addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" which requires the inspection system to examine physically the travel document and optionally to implement and to perform Active Authentication to verify the Authenticity of the presented travel document's chip; the Basic Inspection System to implement the Basic Access Control; and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** "Protection of data from the logical travel document" require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

5 Extended Components Definition

This security target uses the components defined as extensions to CC part 2. The extended components are as defined in chapter 5 of EAC PP ([PP-0056]) which in turn uses extended components defined in PACE PP ([PP-0068]):

- FIA_API Authentication Proof of Identity defined in sec. 5.1 of EAC PP
- FAU_SAS Audit data storage defined in sec. 5.1 of PACE PP
- FCS_RND Generation of random numbers defined in sec. 5.2 of PACE PP
- FMT_LIM Limited capabilities and availability defined in sec. 5.3 of PACE PP
- FPT_EMS TOE emanation defined in sec. 5.4 of PACE PP

These definitions are taken over as described in ([PP-0056]) and ([PP-0068]), and therefore they are not repeated here.

6 Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and *iteration* are defined in paragraph C.4 of Part 1 ([CC_P1]) 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. Refinement of security requirements is denoted by the word “refinement” in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, the words are ~~crossed out~~.

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

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

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

The definition of the subjects “Manufacturer”, “Personalisation Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from ([CC_P2]). The operation “load” is synonymous to “import” used in ([CC_P2]).

Definition of security attributes:

Table 14: Security attributes.

Security Attribute	Values	Meaning
Terminal authentication status	None (any Terminal)	Default role (i.e. without authorisation after start-up)
	CVCA	Roles defined in the certificate used for authentication ([TR-03110]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	Roles defined in the certificate used for authentication ([TR-03110]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1

	DV (foreign)	Roles defined in the certificate used for authentication ([TR-03110]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	Roles defined in the certificate used for authentication ([TR-03110]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	None	
	DG4 (Iris)	Read access to DG4: ([TR-03110])
	DG3 (Fingerprint)	Read access to DG3: ([TR-03110])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: ([TR-03110])

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

Table 15: Keys and certificates.

Name	Data
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate ([TR-03110]). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.

Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 ([ISO_11770-3]).
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Active Authentication Public Key Pair	The Active Authentication Public Key Pair (SK_{AA}, PK_{AA}) are used for Active Authentication according to ([ICAO]).
Active Authentication Public Key (PK_{AA})	The Active Authentication Public Key (PK_{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.
Active Authentication Private Key (SK_{AA})	The Active Authentication Private Key (SK_{AA}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organisation signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organisation with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

Note 8: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's point of view the domestic Document Verifier belongs to the issuing State or Organisation.

6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

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

6.1.1 CLASS FCS CRYPTOGRAPHIC SUPPORT

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

6.1.1.1 CRYPTOGRAPHIC KEY GENERATION (FCS_CKM.1)

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (Table 16)[1] and specified cryptographic key sizes (Table 16)[2] that meet the following: based on an ECDH protocol compliant to ([TR-03111])[3].

Table 16: FCS_CKM.1/CA assignments.

Type	Cryptographic key algorithm	Cryptographic key sizes
ECDH-3DES	ECDH key agreement – 192, 224, 256, 320, 384, 512 and 521 bits	112 bits
ECDH-AES		128, 192, and 256 bits

Note 9: FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to ([TR-03110]).

Note 10: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see ([TR-03110]). This protocol is based on ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) ([TR-03111]). The shared secret value is used to derive the Chip Authentication Session Keys used for encryption and MAC computation for secure messaging (defined in Key Derivation Function ([TR-03110])).

Note 11: The TOE shall implement 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 v.1 may use SHA-1 ([TR-03110]). The TOE

[1] [assignment: *cryptographic key generation algorithm*]
[2] [assignment: *cryptographic key sizes*]
[3] [selection: *based on the Diffie-Hellman key derivation protocol compliant to* ([PKCS#3]) *and* ([TR-03110]), *based on an ECDH protocol compliant to* ([TR-03111])]

may implement additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol v.1 (([TR-03110]) for details).

Note 12: The TOE shall destroy any session keys in accordance with FCS_CKM.4 from ([PP-0068]) after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA.

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

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ DH_PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDH compliant to ([TR-03111])[4] and specified cryptographic key sizes (Table 17)[5] that meet the following: ([ICAO]).

Table 17: FCS_CKM.1/DH_PACE assignments.

Type	Cryptographic key algorithm	Cryptographic key sizes
ECDH-3DES	ECDH key agreement – 192, 224, 256, 320, 384, 512 and 521 bits	112 bits
ECDH-AES		128, 192, and 256 bits

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

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

FCS_CKM. 4 Cryptographic key destruction – Session keys

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

[4] [selection: *Diffie- Hellman-Protocol compliant to PKCS#3, ECDH compliant to* ([TR-03111])]
[5] [*assignment: cryptographic key sizes*]

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the volatile memory[6] that meets the following: none[7].

Note 15: The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

6.1.1.2 CRYPTOGRAPHIC OPERATION (FCS_COP.1)

FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ CA_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm (Table 18)[8] and cryptographic key sizes (Table 18)[9] that meet the following: ISO/IEC 10116:2006 ([ISO_10116])[10].

Table 18: FCS_COP.1/CA_ENC assignments.

Type	Cryptographic algorithm	Cryptographic key sizes
3DES	3DES in CBC mode	112 bits
AES	AES in CBC mode	128, 192, and 256 bits

Note 16: This SFR requires the TOE to implement 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.

FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

[6] [*assignment: cryptographic key destruction method*]
[7] [*assignment: list of standards*]
[8] [assignment: *cryptographic algorithm*]
[9] [assignment: *cryptographic key sizes*]
[10] [assignment: *list of standards*]

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ECDSA with SHA-224, SHA-256, SHA-384 or SHA-512[11] and cryptographic key sizes 192, 224, 256, 320, 384, 512 and 521 bits[12] that meet the following: ([TR-03111])[13].

FCS_COP.1/CA_MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ CA_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm (Table 19)[14] and cryptographic key sizes (Table 19)[15] that meet the following: list of standards (Table 19)[16].

Table 19: FCS_COP.1.1/CA_MAC assignments.

Type	Cryptographic algorithm	Cryptographic key sizes	List of standards
3DES	3DES Retail-MAC	112 bits	ISO/IEC 9797-1
AES	AES CMAC	128, 192, and 256 bits	NIST SP800-38B

Note 17: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication 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 authentication mechanism.

FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES / 3DES

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1.1/ PACE_ENC	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm AES and 3DES[17] in CBC mode and cryptographic key sizes (Table 20)[18] that meet the following: compliant to ([ICAO]).

Table 20: FCS_COP.1/PACE_ENC assignments.

Type	Cryptographic algorithm	Cryptographic key sizes
3DES	3DES in CBC mode	112 bits
AES	AES in CBC mode	128, 192, and 256 bits

Note 18: This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{Enc}).

FCS_COP.1/PACE_MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ PACE_MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm CMAC and Retail-MAC[19] and cryptographic key sizes (Table 21)[20] that meet the following: compliant to ([ICAO]).

Table 21: FCS_COP.1/PACE_MAC assignments.

Type	Cryptographic algorithm	Cryptographic key sizes
3DES	3DES Retail-MAC	112 bits
AES	AES CMAC	128, 192, and 256 bits

Note 19: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-K_{MAC}). Note that in accordance with ([ICAO]) the (two-key) Triple-DES could be used in Retail mode for secure messaging.

FCS_COP.1/AA Cryptographic operation – AA signature creation by travel document

Hierarchical to:	No other components.

[17] [selection: *AES, 3DES*]
[18] [selection: *112, 128, 192, 256*]
[19] [selection: *CMAC, Retail-MAC*]
[20] [selection: *112, 128, 192, 256*]

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AA	The TSF shall perform digital signature creation[21] in accordance with a specified cryptographic algorithm RSA with SHA-1[22] and cryptographic key sizes 1024, 1280, 1536 and 2048[23] that meet the following: ([PKCS_1])[24].

6.1.1.3 RANDOM NUMBER GENERATION (FCS_RND.1)

FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet ([AIS-31])[25].

Note 20: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

6.1.2 CLASS FIA IDENTIFICATION AND AUTHENTICATION

Table 22 provides an overview on the authentication mechanisms used.

Table 22: Overview of authentication SFRs.

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

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]
[25] [assignment: *a defined quality metric*]

Note the Chip Authentication Protocol Version 1 as defined in this protection profile 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 v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

6.1.2.1 USER IDENTIFICATION (FIA_UID)

FIA_UID.1/PACE Timing of identification

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 ([ICAO]), 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS 4. to carry out the Chip Authentication Protocol v.1 according to ([TR-03110]) 5. to carry out the Terminal Authentication Protocol v.1 according to ([TR-03110]) 6. none[26]. 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.

Note 21: 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

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

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

Note 22: 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).

Note 23: 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).

6.1.2.2 USER AUTHENTICATION (FIA_UAU)

FIA_UAU.1/PACE Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1/PACE	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to ([ICAO]), 3. to read the Initialization 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 v.1 according to ([TR-03110]) 6. to carry out the Terminal Authentication Protocol v.1 according to ([TR-03110]) 7. none[27]. on behalf of the user to be performed before the user is identified.
FIA_UAU.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.

Note 24: 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 another authorised person or device (BIS-PACE).

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

If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1/PACE	The TSF shall prevent reuse of authentication data related to 1. PACE Protocol according to ([ICAO]), 2. Authentication Mechanism based on Triple-DES[28], 3. Terminal Authentication Protocol v.1 according to ([TR-03110]).

Note 25: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.5.1/PACE	The TSF shall provide 1. PACE Protocol according to ([ICAO]), 2. Passive Authentication according to ([ICAO]) 3. Secure messaging in MAC-ENC mode according to ([ICAO]), 4. Symmetric Authentication Mechanism based on Triple-DES[29], 5. Terminal Authentication Protocol v.1 according to ([TR-03110]) 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 Access Control SFP with Personalisation Agent Key(s)[30].

[28] [selection: *Triple-DES, AES or other approved algorithms*]
[29] [selection: *Triple-DES, AES or other approved algorithms*]
[30] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]

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 v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1.
5. None[31].

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1/EAC	The TSF shall re-authenticate the user under the condition 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.

Note 29: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in ([ICAO]) 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_UAU.6/PACE Re-authenticating of Terminal by the TOE

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

Note 37: The PACE protocol specified in ([ICAO]) starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure

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

messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

6.1.2.3 AUTHENTICATION PROOF OF IDENTITY (FIA_API.1)

FIA_API.1/CA Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/CA	The TSF shall provide a Chip Authentication Protocol Version 1 according to ([TR-03110]) to prove the identity of the TOE.

Note 30: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in ([TR-03110]). The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to ([ICAO]). The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/AA	The TSF shall provide an Active Authentication Mechanism according to ([ICAO])[32] to prove the identity of the TOE[33].

Note 31: This SFR requires the TOE to implement the Active Authentication Mechanism specified in ([ICAO]). The terminal generates a random challenge which is then signed by the TOE using the Active Authentication Private Key. The terminal verifies the signature using the corresponding Active Authentication Public Key (EF.DG15) to prove the authenticity of the TOE.

6.1.2.4 AUTHENTICATION FAILURES (FIA_AFL)

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

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1/PACE	The TSF shall detect when one[34] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password.

[32] [assignment: *authentication mechanism*]
[33] [assignment: *authorized user or role*]
[34] [assignment: *positive integer number*]

FIA_AFL.1.2/PACE	When the defined number of unsuccessful authentication attempts has been met, the TSF shall consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords[35].

6.1.3 CLASS FDP USER DATA PROTECTION

6.1.3.1 ACCESS CONTROL POLICY (FDP_ACC)

FDP_ACC.1/TRM Subset access control

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

6.1.3.2 ACCESS CONTROL FUNCTIONS (FDP_ACF)

FDP_ACF.1/TRM Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1/ TRM	The TSF shall enforce the Access Control SFP 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 3. Security attributes: a. PACE Authentication b. Terminal Authentication v.1 c. Authorisation of the Terminal.

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

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to ([ICAO]) after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

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

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

Note 32: The relative certificate holder authorization encoded in the CVC of the inspection system is defined in ([TR-03110]). 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.

Note 33: Please note that the Document Security Object (SO_D) stored in EF.SOD (see ([ICAO])) 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 ([ICAO]).

Note 34: 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 Password Authenticated Connection Establishment, and the Chip Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

6.1.3.3 RESIDUAL INFORMATION PROTECTION (FDP_RIP)

FDP_RIP.1 Subset residual information protection

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[36] 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), 3. none[37].

6.1.3.4 INTER-TSF USER DATA CONFIDENTIALITY TRANSFER PROTECTION (FDP_UCT)

FDP_UCT.1/TRM Basic data exchange confidentiality – MRTD

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/TRM	The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

6.1.3.5 INTER-TSF USER DATA INTEGRITY TRANSFER PROTECTION (FDP_UIT)

FDP_UIT.1/TRM Data exchange integrity

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

[36] [selection: *allocation of the resource to, deallocation of the resource from*]
[37] [assignment: *list of objects*]

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

6.1.3.6 IMPORT FROM OUTSIDE OF THE TOE (FDP_ITC)

FDP_ITC.1 Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1	The TSF shall enforce the Access Control SFP[38] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: secret cryptographic keys shall be encrypted[39].

6.1.4 CLASS FMT SECURITY MANAGEMENT

6.1.4.1 SPECIFICATION OF MANAGEMENT FUNCTIONS (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

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

6.1.4.2 SECURITY MANAGEMENT ROLES (FMT_SMR)

Note 35: The SFR FMT_SMR.1/PACE provides basic requirements to the management of the TSF data.

FMT_SMR.1/PACE Security roles

Hierarchical to:	No other components.

[38] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[39] [assignment: *additional importation control rules*]

Dependencies:	FIA_UID.1 Timing of identification.
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.
FMT_SMR.1.2/ PACE	The TSF shall be able to associate users with roles.

6.1.4.3 LIMITED CAPABILITIES AND AVAILABILITY (FMT_LIM)

Note 36: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

FMT_LIM.1 Limited capabilities

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow, 1. User Data to be 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.

FMT_LIM.2 Limited availability

Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow: 1. User Data to be 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.

Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

6.1.4.4 MANAGEMENT OF TSF DATA (FMT_MTD)

Note 40: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ CVCA_INI	The TSF shall restrict the ability to write the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date, 4. none[40]. to the Personalization Agent[41].

Note 41: The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifying Certification Authority Public Key, 2. Country Verifying Certification Authority Certificate to Country Verifying Certification Authority.

Note 42: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key by means of the Country Verifying CA Link-Certificates ([TR-03110]).

[40] [assignment: *list of TSF data*]
[41] [assignment: *the authorised identified roles*]

The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal ([TR-03110]).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ DATE	The TSF shall restrict the ability to modify the Current date to 1. Country Verifying Certification Authority, 2. Document Verifier, 3. Domestic Extended Inspection System.

Note 43: The authorized roles are identified in their certificate ([TR-03110]) 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 ([TR-03110]).

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ CAPK	The TSF shall restrict the ability to load[42] the Chip Authentication Private Key to the Personalization Agent[43].

Note 44: The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

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

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ AAPK	The TSF shall restrict the ability to load[44] the Active Authentication Private Key[45] to the Personalization Agent[46].

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

Hierarchical to:	No other components.

[42] [selection: *create, load*]
[43] [assignment: *the authorised identified roles*]
[44] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[45] [assignment: *list of TSF data*]
[46] [assignment: *the authorised identified roles*]

Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ KEY_READ	The TSF shall restrict the ability to read the 1. PACE passwords, 2. Chip Authentication Private Key, 3. Personalisation Agent Keys, 4. **refinement: Active Authentication Private Key**[47] to none.

FMT_MTD.1/INI_ENA Management of TSF data – Writing Initialisation and Pre-personalisation Data

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MTD.1.1/ INI_ENA	The TSF shall restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.

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

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

Note 45: 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/PA Management of TSF data – Personalisation Agent

Hierarchical to:	No other components.
Dependencies:	FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1 FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

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

FMT_MTD.1.1/ PA	The TSF shall restrict the ability to write the Document Security Object (SO_D) to the Personalisation Agent.

Note 46: 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

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control.

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.

Note 45: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

6.1.5 CLASS FPT PROTECTION OF THE SECURITY FUNCTIONS

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit variations in the power consumption, the timing of signals and the electromagnetic radiation[48] in excess of intelligible limits[49] enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem-SK_{PICC}-PACE,
4. Active Authentication Private Key[50],
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key and
7. none[51].

FPT_EMS.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts 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. Active Authentication Private Key[52],
5. Personalisation Agent Key(s) and
6. Chip Authentication Private Key and
7. none[53].

Note 46: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to ISO/IEC 7816-2 ([ISO_7816]) 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

Hierarchical to: No other components.

[48] [*assignment: types of emissions*]
[49] [assignment: *specified limits*]
[50] [assignment: *list of types of TSF data*]
[51] [assignment: *list of types of user data*]
[52] [assignment: *list of types of TSF data*]
[53] [assignment: *list of types of user data*]

Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: 1. Exposure to operating conditions causing a TOE malfunction, 2. Failure detected by TSF according to FPT_TST.1, 3. none[54].

FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self-tests during initial start-up and periodically during normal operation at the conditions random number generation, cryptographic computation and update of TSF data[55] to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

FPT_PHP.3 Resistance to physical attack

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

Note 47: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

6.1.6 CLASS FTP TRUSTED PATH/CHANNELS

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

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

[54] [assignment: *list of types of failures in the TSF*]
[55] [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]

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.

Note 48: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE.

Note 49: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM.

6.1.7 CLASS FAU SECURITY AUDIT

FAU_SAS.1 Audit storage

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

Note 50: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase ‘manufacturing’. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

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

Note 51: The TOE shall protect the assets against high attack potential. This includes intermediate storage in the chip as well as secure channel communications established using the Chip Authentication Protocol v.1 (OE.Prot_Logical_Travel_Document). If the TOE is operated in non-certified mode using the BAC-established communication channel, the confidentiality of the standard data shall be protected against attackers with at least Enhanced-Basic attack potential (AVA_VAN.3).

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following table provides an overview for security functional requirements coverage.

Table 23: Coverage of Security Objective for the TOE by SFR.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FAU_SAS.1				x				x					
FCS_CKM.1/DH_PACE					x	x	x						
FCS_CKM.1/CA	x	x		x	x	x	x						
FCS_CKM.4	x			x	x	x	x						
FCS_COP.1/PACE_ENC							x						
FCS_COP.1/CA_ENC	x	x		x	x		x						
FCS_COP.1/PACE_MAC					x	x							
FCS_COP.1/CA_MAC	x	x		x	x								
FCS_COP.1/SIG_VER	x			x									
FCS_COP.1/AA			x										
FCS_RND.1	x			x	x	x	x						
FIA_AFL.1/PACE											x		
FIA_UID.1/PACE	x			x	x	x	x						
FIA_UAU.1/PACE	x			x	x	x	x						
FIA_UAU.4/PACE	x			x	x	x	x						
FIA_UAU.5/PACE	x			x	x	x	x						
FIA_UAU.6/PACE					x	x	x						
FIA_UAU.6/EAC	x			x	x	x	x						
FIA_API.1/CA		x											
FIA_API.1/AA			x										

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.Active_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction
FDP_ACC.1/TRM	x			x	x		x						
FDP_ACF.1/TRM	x			x	x		x						
FDP_RIP.1					x	x	x						
FDP_UCT.1/TRM	x				x		x						
FDP_UIT.1/TRM					x		x						
FDP_ITC.1			x										
FMT_SMF.1		x	x	x	x	x	x	x					
FMT_SMR.1/PACE		x	x	x	x	x	x	x					
FMT_LIM.1									x				
FMT_LIM.2									x				
FMT_MTD.1/INI_ENA				x				x					
FMT_MTD.1/INI_DIS				x				x					
FMT_MTD.1/CVCA_INI	x												
FMT_MTD.1/CVCA_UPD	x												
FMT_MTD.1/DATE	x												
FMT_MTD.1/CAPK	x	x			x								
FMT_MTD.1/AAPK			x		x								
FMT_MTD.1/PA				x	x	x	x						
FMT_MTD.1/KEY_READ	x	x	x	x	x	x	x						
FMT_MTD.3	x												
FPT_EMS.1				x						x			
FPT_TST.1										x			x
FPT_FLS.1										x			x
FPT_PHP.3					x					x		x	
FTP_ITC.1/PACE					x	x	x				x		

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given in section 6.3 of ([PP-0056]) and ([PP-0068]), with the following changes:

- Replace EAC PP ([PP-0056]) sentence beginning on line 1146 with:

  The SFR FMT_MTD.1/CAPK, FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Private Key and Active Authentication Private Key cannot be written unauthorized or read afterwards.

- Replace EAC PP ([PP-0056]) sentence beginning on line 1206 with:

  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/CA proving the identity of the TOE.

- Add the justification for OT.Active_Auth_Proof as follows:

  The security objective **OT.Active_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Active Authentication Mechanism provided by FIA_API.1/AA proving the identity of the TOE. The Active Authentication Mechanism defined by FCS_COP.1/AA is performed using a TOE internally stored confidential private key as required by FDP.ITC.1, FMT_MTD.1/AAPK and FMT_MTD.1/KEY_READ.

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

6.3.2 DEPENDENCY RATIONALE

The dependency analysis for the SFRs is provided in the EAC PP ([PP-0056]), section 6.3.2, with the following additions:

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	-
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/PACE_ ENC, FCS_COP.1/PACE_ MAC. FCS_CKM.4
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1/CA_ ENC, FCS_COP.1/CA_ MAC. FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/DH_PACE, FCS_CKM.1/CA
FCS_COP.1/PACE_ENC	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4.
FCS_COP.1/CA_ENC	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/CA FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM] FCS_CKM.4	FCS_CKM.1/DH_PACE FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/CA FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/CA FCS_CKM.4
FCS_COP.1/AA	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 Justification no. 1
FCS_RND.1	No dependencies	-

SFR	Dependencies	Support of the Dependencies
FIA_AFL.1/PACE	FIA_UAU.1	FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	-
FIA_UAU.1/PACE	FIA_UID.1	FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	-
FIA_UAU.5/PACE	No dependencies	-
FIA_UAU.6/PACE	No dependencies	-
FIA_UAU.6/EAC	No dependencies	-
FIA_API.1/CA	No dependencies	-
FIA_API.1/AA	No dependencies	-
FDP_ACC.1/TRM	FDP_ACF.1	FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/TRM Justification no. 2
FDP_RIP.1	No dependencies	-
FDP_UCT.1/TRM	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/PACE FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1/PACE FDP_ACC.1/TRM
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/TRM Justification no. 2
FMT_SMF.1	No dependencies	-
FMT_SMR.1/PACE	FIA_UID.1	FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/AAPK	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1	FMT_SMF.1

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1	FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1/CVCA_INI FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	-
FPT_TST.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FTP_ITC.1/PACE	No dependencies	-

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

No. 1 When the Active Authentication Private Key is loaded, it is permanently stored within the TOE. There is no need for FCS_CKM.4.

No. 2 The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

6.3.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The EAL4 was chosen and augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 based on the claimed EAC PP. The rationale for this selection is stated in section 6.3.3 of ([PP-0056]).

6.3.4 SECURITY REQUIREMENTS – MUTUAL SUPPORT AND INTERNAL CONSISTENCY

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

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

The dependency analysis in section 6.3.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-satisfied dependencies are appropriately explained.

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

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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

7 TOE Summary Specification

7.1 TOE SECURITY FUNCTIONS

The TOE is a composite product that consists of the IC and cryptographic library (Platform) and the Embedded Software (Application) which provide the following security functions (TSF).

7.1.1 TOE SECURITY FUNCTION OF IC AND CRYPTOGRAPHIC LIBRARY (PLATFORM)

SF.IC_CryptoLib

This Security Function covers the security functions of the hardware ST31G480 C01 and of the cryptographic library NesLib 4.2.10.

7.1.2 TOE SECURITY FUNCTIONS OF EMBEDDED SOFTWARE (APPLICATION)

Identification and Authentication of Roles (SF.Identification_Authentication)

This TSF implements the following authentication mechanisms:

1. Password-Authenticated Connection Establishment (PACE)
2. Chip Authentication (CA) version 1
3. Terminal Authentication (TA) version 1
4. Active Authentication (AA)
5. Symmetric Authentication Mechanism based on Triple-DES

The first four protocols are as defined by ICAO and the last protocol is as defined by GlobalPlatform.

Successful authentication identifies the Role of the external entity as Extended Inspection System with PACE or Terminal Authentication, or Personalisation Agent. For mechanisms (1), (2) and (5), session keys for encryption and message authentication are established and stored in volatile memory for Secure Messaging. For mechanism (5), a session key for key encryption is established also.

At the end of the authentication protocol or when the secure messaging session is terminated, the memory used to store the respective ephemeral keys or sessions keys is deallocated.

The PACE authentication mechanism includes a delay mechanism that lengthens the processing time of unsuccessful attempts and gradually increases the delay for consecutive failures.

The Symmetric Authentication Mechanism based on Triple-DES allows ten retries. If the retry limit is reached, further authentication with that key version will fail.

Access Control of User Data (SF.Access_Control)

The TOE stores data within three types of files (EF):

- Working EF – for storing User Data, e.g. EF.SOD, EF.DG1, EF.CardAccess, CVCA Certificate.
- Internal EF

- Security Environment EF – for storing authentication mechanism attributes and file references
- Key EF – for storing cryptographic keys

All three types of EFs are created with individual file control parameters, which includes security attributes and life cycle state. The security attributes determine which commands can be used to access the EF under which security level established by prior identification and authentication protocol. Moreover, the life cycle state determines whether the file is always accessible, has restricted access (activated), or not accessible (deactivated or terminated).

In addition, TDES keys for Symmetric Authentication Mechanism used to identify and authenticate the Personalisation Agent are stored in GP Issuer Security Domain (ISD) or Supplementary Security Domains (SSD).

The EF for storing cryptographic keys, ISD and SSD requires secret key or private key components to be loaded in encrypted format and does not allow them to be read out.

Secure Messaging (SF.Secure_Messaging)

This TSF implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The secure messaging algorithms are in accordance with the PACE and Chip Authentication protocols, and with GP Secure Channel Protocol 02 (SCP02).

The session keys are agreed between the TOE and the terminal from prior successful execution of the PACE, Chip Authentication or Secure Channel Protocol 02 authentication.

An error with the MAC will terminate the secure messaging session and alert the TOE to reset the session keys and security level.

Life Cycle Management (SF.Management)

During TOE Manufacturing phase, the ELM Application allows the Manufacturer to write and read Initialisation Data and Pre-personalisation Data, and configure the TOE to restrict or block their access during Personalisation phase and Operational Use phase. Authentication with a password assigned to the Manufacturer is needed to access the ELM commands.

At the end of the Manufacturing phase, the ELM Application is used to lock the TOE to User configuration and the ELM Application must be deleted to disable its functionality and to reclaim its NVM memory space.

Self-protection (SF.Self-protection)

The TOE hardware and cryptographic library provides countermeasures against

- Physical or invasive attacks
- Side-channel attacks
- Fault injection attacks

The ES provides additional countermeasures against:

- Fault injection attacks
- Differential fault attack
- Invalid commands and communication protocols
- Power loss

7.2 TOE SUMMARY SPECIFICATION RATIONALE

The table below shows the coverage of the SFRs by TSFs.

Table 24: Coverage of SFRs by TSFs.

SFR	SF.IC_CryptoLib	SF.Identification_Authentication	SF.Secure_Messaging	SF.Access_Control	SF.Management	SF.Self-protection
FCS_CKM.1/CA	x	x				
FCS_CKM.1/DH_PACE	x	x				
FCS_CKM. 4						
FCS_COP.1/CA_ENC	x		x			
FCS_COP.1/SIG_VER	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/AA	x	x				
FCS_RND.1	x					
FIA_UID.1/PACE	x	x			x	
FIA_UAU.1/PACE	x	x			x	
FIA_UAU.4/PACE	x	x				
FIA_UAU.5/PACE	x	x	x			
FIA_UAU.6/EAC	x		x			
FIA_UAU.6/PACE	x		x			
FIA_API.1/CA	x	x				
FIA_API.1/AA	x	x				
FIA_AFL.1/PACE	x	x				
FDP_ACC.1/TRM				x		
FDP_ACF.1/TRM				x		
FDP_RIP.1		x				

SFR	SF.IC_CryptoLib	SF.Identification_Authentication	SF.Secure_Messaging	SF.Access_Control	SF.Management	SF.Self-protection
FDP_UCT.1/TRM	x		x			
FDP_UIT.1/TRM	x		x			
FDP_ITC.1				x		
FMT_SMF.1	x	x			x	
FMT_SMR.1/PACE	x	x			x	
FMT_LIM.1	x				x	
FMT_LIM.2	x				x	
FMT_MTD.1/CVCA_INI	x	x		x		
FMT_MTD.1/CVCA_UPD	x	x		x		
FMT_MTD.1/DATE	x	x		x		
FMT_MTD.1/CAPK	x	x		x		
FMT_MTD.1/AAPK	x	x		x		
FMT_MTD.1/KEY_READ				x		
FMT_MTD.1/INI_ENA	x				x	
FMT_MTD.1/INI_DIS	x				x	
FMT_MTD.1/PA	x	x		x		
FMT_MTD.3	x	x		x		
FPT_EMS.1	x					x
FPT_FLS.1	x					x
FPT_TST.1	x					x
FPT_PHP.3	x					x
FTP_ITC.1/PACE	x		x			
FAU_SAS.1	x				x	

FCS_CKM.1/CA: The TOE performs the ECDH key agreement algorithm with SHA-1 function to derive Chip Authentication Session Keys used for encryption and MAC computation for secure messaging. Previous session keys are replaced by the new session keys. This SFR is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FCS_CKM.1/DH_PACE: The TOE performs the ECDH key agreement algorithm with SHA-1 or SHA-256 function to derive PACE Session Keys used for encryption and MAC computation for secure

messaging. This SFR is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FCS_CKM. 4: The TOE deallocates the volatile memory used to store the session keys when secure messaging session is terminated. All volatile memory is automatically cleared upon power-on reset. This is performed by SF.Identification_Authentication.

FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC: The TOE performs secure messaging using TDES or AES session keys for encryption and for MAC, respectively, derived by Chip Authentication Protocol Version 1. This is performed by SF.Secure_Messaging and supported by SF.IC_CryptoLib.

FCS_COP.1/SIG_VER: The TOE performs ECDSA signature verification with SHA-2 hashing functions. This function is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC: The TOE performs secure messaging using TDES or AES session keys for encryption and for MAC, respectively, derived by PACE protocol. This is performed by SF.Secure_Messaging and supported by SF.IC_CryptoLib.

FCS_COP.1/AA: The TOE generates digital signature according to PKCS#1. This is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FCS_RND.1: The TOE uses the hardware TRNG to generate the PACE random nonce which is verified by ES according to AIS31 standard. This is performed by SF.IC_CryptoLib.

FIA_UID.1/PACE and FIA_UAU.1/PACE: The TOE allows the user to be authenticated and identified as the Manufacturer, Personalisation Agent and Terminal based on the TOE lifecycle and respective authentication algorithms. This is performed by SF.Management, SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FIA_UAU.4/PACE: The three authentication mechanisms use fresh random data and sequence counter as inputs. This is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FIA_UAU.5/PACE: The TOE performs the authentication mechanisms using SF.Identification_Authentication. When the secure channel and session keys have been established, SF.Secure_Messaging decrypts/encrypts and authenticates/signs the commands and responses. These three SFs are supported by SF.IC_CryptoLib.

FIA_UAU.6/EAC and FIA_UAU.6/PACE: Every secure message as indicated by the CLA byte and during an active secure messaging session is verified in MAC_ENC mode. If the decrypted command and MAC failed the verification, the secure messaging session will be terminated and command will not be processed. This is performed by SF.Secure_Messaging and supported by SF.IC_CryptoLib.

FIA_API.1/CA and FIA_API.1/AA: The TOE implements the Chip Authentication and Active Authentication mechanisms. This is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib.

FIA_AFL.1/PACE: The TOE implements a delay mechanism when PACE authentication failed. The delay is increasingly longer for every consecutive failure. This is performed by SF.Identification_Authentication and SF.Access_Control.

FDP_ACC.1/TRM and FDP_ACF.1/TRM: The User Data is stored in EFs. Access to each EF, including EF.SOD, EF.DG1, EF.DG3 and others, is defined by its security attributes. The security attributes specify the necessary authentication mechanism and user. Cryptographic keys are stored in

designated EFs and secret / private keys are not accessible. These functions are performed by SF.Access_Control.

FDP_RIP.1: The TOE deallocates the volatile memory used to store the Session Keys and ephemeral PACE private key. This is performed by SF.Identification_Authentication.

FDP_UCT.1/TRM and FDP_UIT.1/TRM: The TOE controls the secure channel established according to Access Control SFP which utilises MAC_ENC mode. Commands and User Data are protected from disclosure, modification, deletion, insertion and replay. This is performed by SF.Secure_Messaging and supported by SF.IC_CryptoLib.

FDP_ITC.1: The TOE enforces the access security attributes of each EF. Secret cryptographic keys must be encrypted with session key when written into the EF. This function is performed by SF.Access_Control.

FMT_SMF.1: The TOE implements an Early Lifecycle Manager (SF.Management) which controls the Initialisation, Pre-personalisation and Configuration functions. The Personalisation function is managed by the rest of the TOE (SF.Identification_Authentication). This is supported by SF.IC_CryptoLib.

FMT_SMR.1/PACE: The TOE implements an Early Lifecycle Manager (SF.Management) which maintains the role of the Manufacturer whereas the other roles are maintained by SF.Identification_Authentication. This function is supported by SF.IC_CryptoLib.

FMT_LIM.1 and FMT_LIM.2: The TOE implements an Early Lifecycle Manager which is active during the Manufacturing phase only, i.e. before User Data is loaded. The Early Lifecycle Manager is deleted at the end of the Manufacturing phase and there is no further access to Test Features. This is performed by SF.Management and supported by SF.IC_CryptoLib.

FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/AAPK, FMT_MTD.1/PA and FMT_MTD.3: The User Data is stored in EFs. Access to each EF is defined by its security attributes (SF.Access_Control). The security attributes specify the necessary authentication mechanism and user (SF.Identification_Authentication). This is supported by SF.IC_CryptoLib.

FMT_MTD.1.1/KEY_READ: The TOE does not allow read access to EFs designated for keys. This is performed by SF.Access_Control.

FMT_MTD.1/INI_ENA and FAU_SAS.1: The TOE implements an Early Lifecycle Manager which allows the Manufacturer to write the Initialisation Data and Pre-personalisation Data. This is performed by SF.Management and supported by SF.IC_CryptoLib.

FMT_MTD.1/INI_DIS: The TOE blocks the role Manufacturer at the end of the manufacturing phase by deleting the Early Lifecycle Manager. The Initialisation Data and Pre-personalisation Data can be read out by the Personalisation Agent only upon successful execution of the Authentication Mechanism based on Triple-DES. This is performed by SF.Identification_Authentication and supported by SF.IC_CryptoLib. Alternatively, access to the Initialisation Data and Pre-personalisation Data can be blocked via Early Lifecycle Manager configuration (SF.Management).

FPT_EMS.1, FPT_FLS.1, FPT_TST.1 and FPT_PHP.3: The TOE implements the recommended security mechanisms of the Security IC to limit emanations and to activate automatic monitoring of hardware malfunctions and failures. This is performed by SF.Self-protection and SF.IC_CryptoLib.

FTP_ITC.1/PACE: The TOE implements secure messaging in MAC_ENC mode using session keys established by the PACE protocol. This is performed by SF.Secure_Messaging and supported by SF.IC_CryptoLib.

7.3 STATEMENT OF COMPATIBILITY

This statement of compatibility between this Composite Security Target and the ST31G480 Platform Security Target shows, in the form of a mapping, that the Security Targets of the composite product and of the underlying platform match, i.e. that there is no conflict between security environments, security objectives, and security requirements of this Composite Security Target and the ST31G480 Platform Security Target ([ST31G_ST]). This is provided by indicating the concerned elements directly in the Security Target for the composite product followed by explanatory text.

Please note that the MIFARE Plus and DESFire features of the platform are inactive, see Table 1. They will not be considered within this statement of compatibility.

7.3.1 COMPATIBILITY OF TOE SECURITY ENVIRONMENT

This section analyses the compatibility of the assumptions, threats, organisational security policies, security objectives and security requirements between the Composite Security Target and the Platform Security Target.

7.3.1.1 ASSUMPTIONS

This section analyses the compatibility between the assumptions of the Platform and the TOE.

All assumptions by the Platform related to MIFARE Plus and DESFire features are not relevant because these two features are inactive in the composite TOE, see Table 1.

The following assumptions by the Platform are met by the security objectives of the composite TOE:

- A.Process-Sec-IC – Protection during Packaging, Finishing and Personalisation
- A.Resp-Appl – Treatment of User Data of the Composite TOE

All assumptions by the Platform do not contradict the assumptions of the composite TOE.

The following assumptions by the composite TOE do not conflict with the assumptions of the Platform because they concern external entities, i.e. Extended Inspection System, issuing States and receiving States, which are outside the scope of the Platform TOE.

- A.Insp_Sys – Inspection Systems for global interoperability
- A.Auth_PKI – PKI for Inspection Systems
- A.Passive_Auth – PKI for Passive Authentication

7.3.1.2 THREATS

This section analyses the compatibility between the threats to the Platform and the TOE.

All Platform threats related to MIFARE Plus and DESFire features are not relevant because these two features are inactive in the composite TOE, see Table 1.

The following threats to the Platform are mapped to threats to the composite TOE:

- T.Leak-Inherent – Inherent Information Leakage
  - This threat matches T.Information_Leakage of the composite TOE.
- T.Phys-Probing – Physical Probing
  - This threat matches T.Phys-Tamper of the composite TOE.
- T.Malfunction – Malfunction due to Environmental Stress
  - This threat matches T.Malfunction of the composite TOE.
- T.Phys-Manipulation – Physical Manipulation
  - This threat matches T.Phys-Tamper of the composite TOE.
- T.Leak-Forced – Forced Information Leakage
  - This threat matches T.Information_Leakage of the composite TOE.
- T.Abuse-Func – Abuse of Functionality
  - This threat matches T.Abuse-Func of the composite TOE.
- T.RND – Deficiency of Random Numbers
  - This threat is mapped to T.Read_Sensitive_Data, T.Counterfeit, T.Skimming, T.Eavesdropping, T.Tracing, T.Forgery, T.Phys-Tamper and T.Malfunction of the composite TOE because they involve random numbers.

The following threat to the Platform is not relevant to the composite TOE:

- T.Mem-Access – Memory Access Violation
  - The security objective (O.Mem_Access) associated with this threat is not relevant, see section 7.3.1.4.

The following threats to the composite TOE cover all threats to the Platform TOE:

- T.Read_Sensitive_Data – Read the sensitive biometric reference data
  - This threat covers T.RND and T.Mem-Access of the Platform TOE.
- T.Counterfeit – Counterfeit of travel document chip data
  - This threat covers T.RND of the Platform TOE.
- T.Skimming – Skimming travel document / Capturing Card-Terminal Communication
  - This threat covers T.RND of the Platform TOE.
- T.Eavesdropping – Eavesdropping on the communication between the TOE and the PACE terminal
  - This threat covers T.RND of the Platform TOE.
- T.Tracing – Tracing travel document
  - This threat covers T.RND of the Platform TOE.
- T.Forgery – Forgery of Data
  - This threat covers T.RND and T.Mem-Access of the Platform TOE.
- T.Abuse-Func – Abuse of Functionality
  - This threat matches T.Abuse-Func of the Platform TOE.

- T.Information_Leakage – Information Leakage from travel document
    - This threat covers T.Leak-Inherent and T.Leak-Forced of the Platform TOE.
- T.Phys-Tamper – Physical Tampering
    - This threat covers T.Phys-Probing and T.Phys-Manipulation of the Platform TOE.
- T.Malfunction – Malfunction due to Environmental Stress
    - This threat matches T.Malfunction of the Platform TOE.

All threats to the composite TOE are mapped to threats to the Platform as described above. They do not conflict each other.

7.3.1.3 ORGANISATIONAL SECURITY POLICIES

This section analyses the compatibility between the Organisational Security Policies of the Platform and the composite TOE.

All Platform OSPs related to MIFARE Plus and DESFire features are not relevant because these two features are inactive in the composite TOE, see Table 1.

According to the Platform security objectives selected in section 7.3.1.4 below, the relevant Platform OSPs are as follows:

- P.Process-TOE – Identification during TOE Development and Production
- P.Add-Functions – Additional Specific Security Functionality
- P.Lim_Block_Loader – Limiting and Blocking the Loader Functionality

All the relevant OSPs of the Platform are not contradictory to the OSPs of the Composite-TOE.

The compatibility between the relevant organisational security policies of the Platform and the threats to the composite TOE is explained below:

- P.Process-TOE – Identification during TOE Development and Production
    - This OSP does not conflict with T.Tracing of the composite TOE where the unique IC identification is meant for initialisation phase, pre-personalisation phase and personalisation phase only and cannot be used to trace the movement of the travel document during operational phase.
- P.Add-Functions – Additional Specific Security Functionality
    - This OSP helps counter all threats to the composite TOE, except T.Abuse-Func, where the security mechanisms use cryptographic functions. This OSP does not conflict with T.Abuse-Func because the cryptographic functions are meant for use during the TOE operational phase.
- P.Lim_Block_Loader – Limiting and Blocking the Loader Functionality
    - This OSP helps counter T.Abuse-Func of the composite TOE where the Loader functionality is limited to the initialisation phase and is blocked during the personalisation phase and operational phase.

There is no conflict between the relevant organisational security policies of the Platform and the threats to the composite TOE.

7.3.1.4 SECURITY OBJECTIVES FOR THE TOE

This section analyses the compatibility between the security objectives for the Platform TOE and the composite TOE.

All Platform security objectives related to MIFARE Plus and DESFire features are not relevant because these two features are inactive in the composite TOE, see Table 1.

The table below shows the mapping between the remaining security objectives of the Platform and relevant ones of the composite TOE.

Table 25: Mapping between security objectives of the Platform and the TOE.

Platform	TOE												
	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
O.Leak-Inherent									x				
O.Phys-Probing											x		
O.Malfunction												x	
O.Phys-Manipulation											x		
O.Leak-Forced									x				
O.Abuse-Func								x					
O.Identification							x						
O.RND	x		x	x	x	x							
O.Cap-Avail-Loader								x					
O.Add-Functions	x	x	x	x	x	x				x			x
O.Mem-Access													
O.Controlled-ES-Loading													

The following security objectives of the Platform TOE maps to those of the composite TOE:

- O.Leak-Inherent – Protection against Inherent Information Leakage
  - This security objective maps to OT.Prot_Inf_Leak of the composite TOE.
- O.Phys-Probing – Protection against Physical Probing
  - This security objective maps to OT.Prot_Phys-Tamper of the composite TOE.
- O.Malfunction – Protection against Malfunctions
  - This security objective matches OT.Prot_Malfunction of the composite TOE.
- O.Phys-Manipulation – Protection against Physical Manipulation
  - This security objective maps to OT.Prot_Phys-Tamper of the composite TOE.

- O.Leak-Forced – Protection against Forced Information Leakage
    - This security objective maps to OT.Prot_Inf_Leak of the composite TOE.
- O.Abuse-Func – Protection against Abuse of Functionality
    - This security objective maps to OT.Prot_Abuse-Func of the composite TOE.
- O.Identification – TOE Identification
    - This security objective matches OT.Identification of the composite TOE.
- O.RND – Random Numbers
    - This security objective maps to OT.Sens_Data_Conf, OT.AC_Pers, OT.Data_Integrity and OT.Data_Confidentiality of the composite TOE.
- O.Cap-Avail-Loader – Capability and Availability of the Loader
    - This security objective maps to OT.Prot_Abuse-Func of the composite TOE.
- O.Add-Functions – Additional Specific Security Functionality
    - This security objective maps to OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.AC_Pers, OT.Data_Integrity, OT.Data_Authenticity, OT.Data_Confidentiality, OT.Tracing and OT.Active_Auth_Proof of the composite TOE.

The following security objective of the Platform TOE is not relevant to the composite TOE and there is no conflict:

- O.Mem-Access – Dynamic Area based Memory Access Control
    - This security objective is not relevant because this Platform feature is not used in the composite TOE.
- O.Controlled-ES-Loading – Controlled loading of the Security IC Embedded Software
    - This security objective is not relevant because its SFRs are not relevant to composite TOE.

The following security objectives of the composite TOE map to those of the Platform TOE:

- OT.Sens_Data_Conf – Confidentiality of sensitive biometric reference data
    - This security objective maps to O.RND and O.Add-Functions of the Platform TOE.
- OT.Chip_Auth_Proof – Proof of the travel document's chip authenticity
    - This security objective maps to O.Add-Functions of the Platform TOE.
- OT.AC_Pers – Access Control for Personalisation of logical MRTD
    - This security objective maps to O.RND and O.Add-Functions of the Platform TOE.
- OT.Data_Integrity – Integrity of Data
    - This security objective maps to O.RND and O.Add-Functions of the Platform TOE.
- OT.Data_Authenticity – Authenticity of Data
    - This security objective maps to O.RND and O.Add-Functions of the Platform TOE.
- OT.Data_Confidentiality – Confidentiality of Data
    - This security objective maps to O.RND and O.Add-Functions of the Platform TOE.
- OT.Identification – Identification of the TOE
    - This security objective maps to O.Identification of the Platform TOE.
- OT.Prot_Abuse-Func – Protection against Abuse of Functionality
    - This security objective maps to O.Abuse-Func and O.Cap-Avail-Loader of the Platform TOE.

- OT.Prot_Inf_Leak – Protection against Information Leakage
  - This security objective maps to O.Leak-Inherent and O.Leak-Forced of the Platform TOE.
- OT.Tracing – Tracing travel document
  - This security objective maps to O.Add-Functions of the Platform TOE.
- OT.Prot_Phys-Tamper – Protection against Physical Tampering
  - This security objective maps to O.Phys-Probing and O.Phys-Manipulation of the Platform TOE.
- OT.Prot_Malfunction – Protection against Malfunctions
  - This security objective maps to O.Malfunction of the Platform TOE.
- OT.Active_Auth_Proof – Proof of travel document's chip authenticity
  - This security objective maps to O.Add-Functions of the Platform TOE.

7.3.1.5 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section analyses the compatibility between the security objectives for the operational environment of the Platform versus the composite TOE.

All relevant assumptions by the Platform are mapped to the assumptions and security objectives of the composite TOE and there is no conflict. There is no significant assumption to be considered.

7.3.1.6 SECURITY REQUIREMENTS

This section analyses the compatibility between the security requirements of the Platform and the TOE. The relevant Platform-SFRs (RP_SFR) can be mapped to the TOE, see Table 26. A list of irrelevant Platform-SFRs (IP_SFR) not used by the Composite ST is presented later in this section.

The table below shows the mapping between the relevant security requirements of the Platform (RP_SFR) and relevant ones of the Composite TOE. Unmapped SFRs of the Platform SFRs (IP_SFR) and Composite SFRs are not included.

Table 26: Mapping between security requirements of the Platform and the TOE.

Platform	TOE																
	FCS_CKM.1/CA	FCS_CKM.1/DH_PACE	FCS_COP.1/CA_ENC	FCS_COP.1/SIG_VER	FCS_COP.1/CA_MAC	FCS_COP.1/PACE_ENC	FCS_COP.1/PACE_MAC	FCS_COP.1/AA	FCS_RND.1	FMT_SMF.1	FMT_LIM.1	FMT_LIM.2	FPT_EMS.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3	FAU_SAS.1
FRU_FLT.2														x	x	x	
FPT_FLS.1														x		x	
FMT_LIM.1/Test											x						

Platform	TOE																
	FCS_CKM.1/CA	FCS_CKM.1/DH_PACE	FCS_COP.1/CA_ENC	FCS_COP.1/SIG_VER	FCS_COP.1/CA_MAC	FCS_COP.1/PACE_ENC	FCS_COP.1/PACE_MAC	FCS_COP.1/AA	FCS_RND.1	FMT_SMF.1	FMT_LIM.1	FMT_LIM.2	FPT_EMS.1	FPT_FLS.1	FPT_TST.1	FPT_PHP.3	FAU_SAS.1
FMT_LIM.1/Loader											x						
FMT_LIM.2/Test												x					
FMT_LIM.2/Loader												x					
FDP_SDC.1											x	x					
FDP_SDI.2											x	x					
FAU_SAS.1																	x
FPT_PHP.3																x	
FDP_ITT.1													x				
FPT_ITT.1													x				
FDP_IFC.1													x				
FCS_RNG.1									x								
FCS_COP.1/TDES			x		x	x	x										
FCS_COP.1/AES			x		x	x	x										
FCS_COP.1/RSA								x									
FCS_COP.1/ECC	x	x		x													
FCS_COP.1/SHA	x	x		x				x									

The compatibility of the security requirements is described below:

- Relevant security requirements of the Platform (RP_SFR)
  - FRU_FLT.2 – Limited fault tolerance : Mapped to FPT_FLS.1, FPT_TST.1 and FPT_PHP.3 of the Composite ST.
  - FPT_FLS.1 – Failure with preservation of secure state : Mapped FPT_FLS.1 and FPT_PHP.3 of the Composite ST.
  - FMT_LIM.1/Test – Limited capabilities : Mapped to FMT_LIM.1 of the Composite ST.
  - FMT_LIM.1/Loader – Limited capabilities : Mapped to FMT_LIM.1 of the Composite ST.
  - FMT_LIM.2/Test – Limited availability : Mapped to FMT_LIM.2 of the Composite ST.
  - FMT_LIM.2/Loader – Limited availability : Mapped to FMT_LIM.2 of the Composite ST.
  - FDP_SDC1 – Stored data confidentiality : Mapped to FMT_LIM.1 and FMT_LIM.2 of the Composite ST.
  - FDP_SDI.2 – Stored data integrity monitoring and action : Mapped to FMT_LIM.1 and FMT_LIM.2 of the Composite ST.

- FAU_SAS.1 – Audit storage : Mapped to FAU_SAS.1 of the Composite ST.
- FPT_PHP.3 – Resistance to physical attack : Mapped to FPT_PHP.3 of the Composite ST.
- FDP_ITT.1 – Basic internal transfer protection : Mapped to FPT_EMS.1 of the Composite ST.
- FPT_ITT.1 – Basic internal TSF data transfer protection : Mapped to FPT_EMS.1 of the Composite ST.
- FDP_IFC.1 – Subset information flow control : Mapped to FPT_EMS.1 of the Composite ST.
- FCS_RNG.1 – Random number generation : Mapped to FCS_RND.1 of the Composite ST.
- FCS_COP.1/TDES – Cryptographic operation: TDES operation : Mapped to FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC and FCS_COP.1/AA of the Composite ST.
- FCS_COP.1/AES – Cryptographic operation: AES operation : Mapped to FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC and FCS_COP.1/AA of the Composite ST.
- FCS_COP.1/RSA – Cryptographic operation: RSA operation : Mapped to FCS_COP.1/AA of the Composite ST.
- FCS_COP.1/ECC – Cryptographic operation: Elliptic Curves Cryptography operation : Mapped to FCS_CKM.1/CA, FCS_CKM.1/DH_PACE and FCS_COP.1/SIG_VER of the Composite ST.
- FCS_COP.1/SHA – Cryptographic operation: SHA operation : Mapped to FCS_CKM.1/CA, FCS_CKM.1/DH_PACE, FCS_COP.1/SIG_VER and FCS_COP.1/AA of the Composite ST.

- Irrelevant security requirements of the Platform (IP_SFR)
  - FCS_COP.1/DRBG – Cryptographic operation: DRBG operation
  - FCS_COP.1/Keccak – Cryptographic operation: Keccak operation
  - FCS_COP.1/Keccak-p – Cryptographic operation: Keccak-p operation
  - FCS_COP.1/Diffie-Hellman – Cryptographic operation: Diffie-Hellman operation
  - FCS_CKM.1/Prime_generation – Cryptographic key generation: Prime generation
  - FCS_CKM.1/RSA_key_generation – Cryptographic key generation: RSA key generation
  - FMT_MSA.1/Memories – Management of security attribute
  - FMT_MSA.3/Memories – Static attribute initialisation
  - FMT_SMF.1/Memories – Specification of management functions
  - FDP_ACC.2/Memories – Complete access control
  - FDP_ACF.1/Memories – Security attribute based access control
  - FMT_MSA.3/Loader – Static attribute initialisation
  - FMT_MSA.1/Loader – Management of security attribute
  - FMT_SMF.1/Loader – Specification of management functions
  - FDP_ACC.1/Loader – Subset access control
  - FDP_ACF.1/Loader – Security attribute based access control
  - FMT_SMR.1/Loader – Security roles
  - FIA_UID.1/Loader – Timing of identification

- FDP_ITC.1/Loader – Import of user data without security attributes
- FMT_SMR.1 / MFPlus – Security roles
- FDP_ACC.1 / MFPlus – Subset access control
- FDP_ACF.1 / MFPlus – Security attribute based access control
- FMT_MSA.3 / MFPlus – Static attribute initialisation
- FMT_MSA.1 / MFPlus – Management of security attributes
- FMT_SMF.1 / MFPlus – Specification of Management Functions
- FDP_ITC.2 / MFPlus – Import of user data with security attributes
- FPT_TDC.1 / MFPlus – Inter-TSF basic TSF data consistency
- FCS_CKM.4 / MFPlus – Cryptographic key destruction
- FIA_UID.2 / MFPlus – User identification before any action
- FIA_UAU.2 / MFPlus – User authentication before any action
- FIA_UAU.5 / MFPlus – Multiple authentication mechanisms
- FMT_MTD.1 / MFPlus – Management of TSF data
- FTP_TRP.1 / MFPlus – Trusted path
- FPT_RPL.1 / MFPlus – Replay detection
- FPR_UNL.1 / MFPlus – Unlinkability
- FRU_RSA.2 / MFPlus – Minimum and maximum quotas
- FDP_RIP.1 / MFPlus – Subset residual information protection
- FMT_SMR.1 / DESFire – Security roles
- FDP_ACC.1 / DESFire – Subset access control
- FDP_ACF.1 / DESFire – Security attribute based access control
- FMT_MSA.3 / DESFire – Static attribute initialisation
- FMT_MSA.1 / DESFire – Management of security attributes
- FMT_SMF.1 / DESFire – Specification of Management Functions
- FDP_ITC.2 / DESFire – Import of user data with security attributes
- FPT_TDC.1 / DESFire – Inter-TSF basic TSF data consistency
- FCS_CKM.4 / DESFire – Cryptographic key destruction
- FIA_UID.2 / DESFire – User identification before any action
- FIA_UAU.2 / DESFire – User authentication before any action
- FIA_UAU.5 / DESFire – Multiple authentication mechanisms
- FMT_MTD.1 / DESFire – Management of TSF data
- FTP_TRP.1 / DESFire – Trusted path
- FDP_ROL.1 / DESFire – Basic rollback
- FPT_RPL.1 / DESFire – Replay detection
- FPR_UNL.1 / DESFire – Unlinkability
- FRU_RSA.2 / DESFire – Minimum and maximum quotas
- FDP_RIP.1 / DESFire – Subset residual information protection
- FDP_ACC.1/APPLI_FWL – Subset access control
- FDP_ACF.1/APPLI_FWL – Security attribute based access control
- FMT_MSA.3/APPLI_FWL – Static attribute initialisation

- Security requirements of the Composite TOE

- FCS_CKM.1/CA – Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys : Mapped to FCS_COP.1/ECC and FCS_COP.1/SHA of the Platform ST.
- FCS_CKM.1/DH_PACE – Cryptographic key generation – Diffie-Hellman for PACE session keys : Mapped to FCS_COP.1/ECC and FCS_COP.1/SHA of the Platform ST.
- FCS_CKM. 4 – Cryptographic key destruction – Session keys : No conflict
- FCS_COP.1/CA_ENC – Cryptographic operation – Symmetric Encryption / Decryption : Mapped to FCS_COP.1/TDES and FCS_COP.1/AES of the Platform ST.
- FCS_COP.1/SIG_VER – Cryptographic operation – Signature verification by travel document : Mapped to FCS_COP.1/ECC and FCS_COP.1/SHA of the Platform ST.
- FCS_COP.1/CA_MAC – Cryptographic operation – MAC : Mapped to FCS_COP.1/TDES and FCS_COP.1/AES of the Platform ST.
- FCS_COP.1/PACE_ENC – Cryptographic operation – Encryption / Decryption AES / 3DES : Mapped to FCS_COP.1/TDES and FCS_COP.1/AES of the Platform ST.
- FCS_COP.1/PACE_MAC – Cryptographic operation – MAC : Mapped to FCS_COP.1/TDES and FCS_COP.1/AES of the Platform ST.
- FCS_COP.1/AA – Cryptographic operation – AA signature creation by travel document : Mapped to FCS_COP.1/RSA and FCS_COP.1/SHA of the Platform ST.
- FCS_RND.1 – Quality metric for random numbers : Mapped to FCS_RNG.1 of the Platform ST.
- FIA_UID.1/PACE – Timing of identification : No conflict.
- FIA_UAU.1/PACE – Timing of authentication : No conflict.
- FIA_UAU.4/PACE – Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE : No conflict.
- FIA_UAU.5/PACE – Multiple authentication mechanisms : No conflict.
- FIA_UAU.6/EAC – Re-authenticating – Re-authenticating of Terminal by the TOE : No conflict.
- FIA_UAU.6/PACE – Re-authenticating of Terminal by the TOE : No conflict.
- FIA_API.1/CA – Authentication Proof of Identity : No conflict.
- FIA_API.1/AA – Authentication Proof of Identity : No conflict.
- FIA_AFL.1/PACE – Authentication failure handling – PACE authentication using non-blocking authorisation data : No conflict.
- FDP_ACC.1/TRM – Subset access control : No conflict.
- FDP_ACF.1/TRM – Security attribute based access control : No conflict.
- FDP_RIP.1 – Subset residual information protection : No conflict.
- FDP_UCT.1/TRM – Basic data exchange confidentiality – MRTD : No conflict.
- FDP_UIT.1/TRM – Data exchange integrity : No conflict.
- FDP_ITC.1 – Import of user data without security attributes : No conflict.
- FMT_SMF.1 – Specification of Management Functions : No conflict.
- FMT_SMR.1/PACE – Security roles : No conflict.
- FMT_LIM.1 – Limited capabilities : Mapped to FMT_LIM.1/Test, FMT_LIM.1/Loader, FDP_SDC.1 and FDP_SDI.2 of the Platform ST.
- FMT_LIM.2 – Limited availability : Mapped to FMT_LIM.2/Test, FMT_LIM.2/Loader, FDP_SDC.1 and FDP_SDI.2 of the Platform ST.

- FMT_MTD.1/CVCA_INI – Management of TSF data – Initialization of CVCA Certificate and Current Date : No conflict.
- FMT_MTD.1/CVCA_UPD – Management of TSF data – Country Verifying Certification Authority : No conflict.
- FMT_MTD.1/DATE – Management of TSF data – Current date : No conflict.
- FMT_MTD.1/CAPK – Management of TSF data – Chip Authentication Private Key : No conflict
- FMT_MTD.1/AAPK – Management of TSF data – Active Authentication Private Key : No conflict.
- FMT_MTD.1/KEY_READ – Management of TSF data – Key Read : No conflict.
- FMT_MTD.1/INI_ENA – Management of TSF data – Writing Initialisation and Pre-personalisation Data : No conflict.
- FMT_MTD.1/INI_DIS – Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data : No conflict.
- FMT_MTD.1/PA – Management of TSF data – Personalisation Agent : No conflict
- FMT_MTD.3 – Secure TSF data : No conflict.
- FPT_EMS.1 – TOE Emanation : Mapped to FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 of the Platform ST.
- FPT_FLS.1 – Failure with preservation of secure state : Mapped to FRU_FLT.2 and FPT_FLS.1 of the Platform ST.
- FPT_TST.1 – TSF testing : Mapped to FRU_FLT.2 of the Platform ST.
- FPT_PHP.3 – Resistance to physical attack : Mapped to FRU_FLT.2, FPT_FLS.1 and FPT_PHP.3 of the Platform ST.
- FTP_ITC.1/PACE – Inter-TSF trusted channel after PACE : No conflict.
- FAU_SAS.1 – Audit storage : Mapped to FAU_SAS.1 of the Platform ST.

7.3.1.7 ASSURANCE REQUIREMENTS

The level of assurance of the TOE is EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5.

The level of assurance of the Platform is EAL 5 augmented by ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5.

Therefore, the assurance requirements of the TOE are exceeded by the assurance requirements of the Platform. There are no conflicts.

7.3.2 CONCLUSION

In conclusion, this security target is compatible with the security target of the Platform ([ST31G_ST]).

8 Glossary and Acronyms

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [5].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [4], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [6] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organisation.
Basic Access Control (BAC)	Security mechanism defined in [6] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
Biographic data (biodata).	The personalised details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [6]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.

Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [6]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [6], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [5].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [5]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organisational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [5].
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Card Verifiable Certificate according to [5].
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [6] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Details Data	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the

	travel document's chip. It may carry the Document Signer Certificate (CDS). [6]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [5] and [6]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [5]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this PP. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [6]
Travel document (electronic)	The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
ePassport application	Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes • the file structure implementing the LDS ([ICAO]), • the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and • the TSF Data including the definition the authentication data but except the authentication data itself.
Extended Access Control	Security mechanism identified in [6] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organisation to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [6]

Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel documents. [6]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [6]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [6]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Inspection	The act of a State examining a travel document presented to it by a traveler (the travel document holder) and verifying its authenticity. [6]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining a travel document presented by the traveler and verifying its authenticity and (ii) verifying the traveler as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organisation
Issuing Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [6]
Issuing State	The Country issuing the travel document. [6]

Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the travel document's chip.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [6] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1. personal data of the 2. travel document holder 3. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 4. the digitized portraits (EF.DG2), 5. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 6. the other data according to LDS (EF.DG5 to EF.DG16). 7. EF.COM and EF.SOD
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [6]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [6] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [6]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [5]. The metadata of a CV certificate comprise the following elements: • Certificate Profile Identifier, • Certificate Authority Reference, • Certificate Holder Reference, • Certificate Holder Authorisation Template, • Certificate Effective Date, • Certificate Expiration Date.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [4],. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE Password	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [4].
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the “Enrolment” (cf. sec. 1.3.3, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [5], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [6] (in the role of DS). Please note that the role ‘Personalisation Agent’ may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i) individual-related data (biographic and biometric data) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing.
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document’s chip to verify the authentication attempt of a terminal

	as Personalisation Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair.
Pre-personalised travel document's chip	Travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the traveler is applying for entry. [6]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [15].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [6]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [14]
Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [4], namely (i) PACE or BAC and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the Travel document and the related value presented to the terminal by the travel document presenter. In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE.

	Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [6] (there "Machine readable travel document").
Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [6], sec III.
Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [5] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE. CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [2]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [6]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
EAC	Extended Access Control
EF	Elementary File
ICCSN	Integrated Circuit Card Serial Number
IP_SFR	Irrelevant Platform SFR
MF	Master File
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
PT	Personalisation Terminal
RF	Radio Frequency
RP_SFR	Relevant Platform SFR
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure
TA	Terminal Authentication
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)

Bibliography

[AIS-31]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** AIS 31, Anwendungshinweise und Interpretationen zum, Version 2.1, 2 December 2011.

[CC_CEM]. **Common Criteria.** CCMB-2017-04-004, Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017.

[CC_P1]. **Common Criteria.** CCMB-2017-04-001, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[CC_P2]. **Common Criteria.** CCMB-2017-04-002, Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[CC_P3]. **Common Criteria.** CCMB-2017-04-003, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

[ICAO]. **International Civil Aviation Organization.** Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015.

[ISO_10116]. **International Organization for Standardization.** ISO/IEC 10116:2006. Information technology − Security techniques − Modes of operation for an n-bit block cipher, 2006.

[ISO_11770-3]. **International Organization for Standardization.** ISO/IEC 11770-3:2015 Information technology -- Security techniques -- Key managemen t-- Part 3: Mechanisms using asymmetric techniques, August 2015.

[ISO_18013]. **International Organization for Standardization.** ISO/IEC 18013 Information technology -- Personal identification -- ISO-compliant driving licence, -.

[ISO_7816]. **International Organization for Standardization.** ISO/IEC 7816 Identification cards - Integrated circuit cards, -.

[MOS_ELM]. **MCS Microsystems Sdn Bhd.** MOS Early Lifecycle Manager Functional Specifications, Version 1.0.0, 2019.

[MOS_FSP]. **MCS Microsystems Sdn Bhd.** MOS - Functional Specifications, Version 1.0.0, 2019.

[MOS_UGD]. **MCS Microsystems Sdn Bhd.** MOS User Guide, Version 1.0.0, 2019.

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

[PKCS_1]. **RSA Laboratory.** PKCS #1, RSA Cryptography Standard, Version 2.1, June 2002.

[PP-0055]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** BSI-CC-PP-0055, Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.10, 25 March 2009.

[PP-0056]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 21 December 2012.

[PP-0068]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** BSI-CC-PP-0068-V2-2011 Common Criteria Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2 November 2011.

[PP-0084]. **Eurosmart.** BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014.

[ST31G_ST]. **STMicroelectronics NV.** ST31G480 C01 including optional cryptographic library NESLIB and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X, Security Target for composition, Common Criteria for IT security evaluation, Rev C01.1, June 2017.

[TR-03110]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Version 2.21, 21 December 2016.

[TR-03111]. **Bundesamt für Sicherheit in der Informationstechnik, Germany.** Technical Guideline TR-03111 Elliptic Curve Cryptography, 17 April 2009.

Confidentiality Obligations

This document contains sensitive information.

Its distribution is subjected to the signature of a Non-Disclosure Agreement.

It is classified “LEVEL 1 - PUBLIC”.

At all times you should comply with the following security rules (refer to NDA for detailed obligations):

Do not copy or reproduce all or part of this document.
Keep this document locked away.

Further copies can be provided on a “need to know basis”. Please contact MCS at the following address.

MCS Microsystems Sdn Bhd
4th Floor,
IRIS Smart Technology Complex,
Technology Park Malaysia, Bukit Jalil,
57000 Kuala Lumpur,
Malaysia.
Tel: 603 – 8996 9168