STMicroelectronics

JSAFE3_EPASS EAC Security Target Public Version

Common Criteria for IT security evaluation

JSAFE3_EPASS_EAC_SecurtyTarget_Lite Rev. A
13 March 2019

life.augmented

BLANK

J JSAFE3_EPASS EAC
Security Target Public Version

Common Criteria for IT Evaluation

1. INTRODUCTION

1.1 Document Reference

Document identification: **JSAFE3_EPASS EAC Security Target - Public Version**
Revision: **A**
Registration: **JSAFE3_EPASS_EAC_SecurtyTarget_Lite**

1.2 Security Target Reference

Document identification: **JSAFE3_EPASS EAC Security Target**
Revision: **I**
Registration: **JSAFE3_EPASS_EAC_SecurtyTarget**

1.3 TOE Reference

TOE Name and Version: JSAFE3_EPASS_EAC V1.0.0

2. PURPOSE

This document presents the Security Target lite of JSAFE3_EPASS_EAC V1.0.0 a contact/contactless chip implementing the machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) [ICAO_9303] and implementing the advanced security methods, Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), Chip Authentication (CA) and the Active Authentication (AA) [ICAO_9303].

This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.

INDEX

Page

List of tables

List of figures

3. REFERENCE DOCUMENTS

CC documents	
[CC_P1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017
[CC_P2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1 Revision 5. April 2017
[CC_P3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004.
[AIS31/20]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, A proposal for Functionality classes for random number generators Version 2.0 vom 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[AIS36]	Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Version 2 vom 12.11.2007, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Protection Profiles and Technical Guidelines	
[PP-0084]	BSI-CC-PP-0084-2014 – Eurosmart – Security IC Platform Protection Profile with Augmentation Packages
[PP-0055]	CC Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control Version 1.10, 25 March 2009
[PP-0056]	CC Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE Version 1.3.2, 05 December 2012
[PP-0068]	CC Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE(PACE PP). BSI-CC-PP-0068-V2-2011 Version 1.0, November 2011
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Seven Edition, 2015 Part 10 Logical Data Structure (LDS) for Storage of Biometric and Other Data in the Contactless Integrated Circuit (IC)
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Seven Edition, 2015 Part 11 Security Mechanisms for MRTDs
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, Seven Edition, 2015 Part 12 Public Key Infrasctucture for MRTDs
[ICAO_TR]	TECHNICAL REPORT Supplemental Access Control for Machine Readable Travel

	Documents Version - 1.1– April 15, 2014
[TR-03110-1]	Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20. March 2012
[TR-03110-2]	Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents Part 2, Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012-03-20
[TR-03110-3]	Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.11, 12. July 2013
[TR-03111]	Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 1.11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009-04-17
Specifications	
[PKCS1_v1_5]	PKCS #1 v1.5: RSA Encryption Standard – RSA Laboratories – 1 Nov 1993
[PKCS_#3]	Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993
[FIPS_46_3]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
[ANSI_X9.62]	ANSI X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA), approved November 16, 2005
[FIPS_180-2]	FIPS Publication 180-2: SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[FIPS_PUB_197]	Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26
[SP800-38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005.
[ISO 10116]	ISO/IEC 10116, Information technology - Security Techniques -- Modes of operation of an n-bit block cipher, ISO, 2006.
[RFC4493]	JH. Song, R. Poovendran The AES-CMAC Algorithm, June 2006
[RFC3447]	NWG Request For Comments 3447 – February 2003
[ISO_9796-2]	ISO/IEC 9796-2:2010 Information technology — Security techniques Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
Platform documents	

[PP_JC_Closed]	Java Card System – Closed Configuration Protection Profile, Version 3.0, December 2012 [ANSSI-CC-PP-2010/07-M01]
[JSAFE3_ST]	JSAFE3 on ST31G480 Security Target
[STLite_ST31G480]	ST31G480 A04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X – Security Target for composition, Rev A04.1 April 2017
[MntRep_ST31G480]	ST31G480 A04 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X – Rapport de manteinance ANSSI-CC-2016/58-M02, June 2017

4. DEFINITIONS

The following tables are taken over from [PP-0055] .

Acronyms

Term	Definition
ATR	Answer To Reset
ATS	*Answer To Select*
AUTH	*External Authentication*
BIS	*Basic Inspection System*
BIS-PACE	*Basic Inspection System with PACE*
CA	*Chip Authentication*
CAN	*Card Access Number*
CC	*Common Criteria for IT Security Evaluation*
CEM	*Common Methodology for Information Technology Security Evaluation*
DF	*Dedicated File*
DPA	*Differential Power Analysis*
EAC	*Extended Access Control*
EAL	*Evaluation Assurance Level*
ECC	*Elliptic Curve Cryptography*
EF	*Elementary File*
Enc	*Encryption*
ENC	*Content Data Encryption*
GIS	*General Inspection System*
HW	*Hardware*
ICCSN	*Integrated Circuit Card Serial Number.*
ID	*Identifier*
IT	*Information Technology*
MF	*Master File*
MRTD	*Machine Readable Travel Document*
MRZ	*Machine readable zone*
n.a.	*Not applicable*
NIST	*National Institute of Standards and Technology*
OSP	*Organizational security policy*
PACE	*Password Authenticated Connection Establishment*
PCD	*Proximity Coupling Device*
PICC	*Proximity Integrated Circuit Chip*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PP	*Protection Profile*
PTRNG	*Physical True Random Number Generator*
PT	*Personalization Terminal*
RF	*Radio Frequency*
RNG	*Random Number Generator*
SAR	*Security Assurance Requirement*
SEMA	*Simple Electromagnetic Analysis*
SF	*Security Function*
SFP	*Security Function Policy*
SFR	*Security Functional Requirement*
SHA	*Secure Hash Algorithm*
SIG	*Content Data Signature*
Sign	*Signature*
SIP	*Standard Inspection Procedure*
SPA	*Simple Power Analysis*
ST	*Security Target*
TA	*Terminal Authentication*
TOE	*Target Of Evaluation*
TRNG	*True Random Number Generator*
TSF	*TOE Security Functionality*

Term	Definition
TSP	*TOE Security Policy (defined by the current document)*

Glossary

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 [TR-03110-1].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [ICAO_TR], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SOD and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [ICAO_9303] 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 [ICAO_9303] 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.
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.

	[ICAO_9303]
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. [ICAO_9303]
Country Signing CA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) 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. [ICAO_9303], 5.5.1. The Country Signing Certification Authority issuing certificates for Document Signers (cf. [ICAO_9303]) 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 [TR-03110-1].
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 [TR-03110-1]. 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 organizational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) 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 [TR-03110-1].
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 [TR-03110-1].
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 [ICAO_9303] 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.

PACE passwords	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 [ICAO_TR],
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 (SOD)	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) [ICAO_9303]
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 [TR-03110-1] and [ICAO_9303]. 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 [TR-03110-1]. 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. [ICAO_9303]
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	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [TR-03110-1].
Extended Access Control	Security mechanism identified in [ICAO_9303] 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	A role of a terminal as part of an inspection system which is in addition
System (EIS)	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. [ICAO_9303]
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. [ICAO_9303]
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. [ICAO_9303]
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. [ICAO_9303]
Initialisation	Process of writing Initialisation Data
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 an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [ICAO_9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller 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). [ICAO_9303]

Issuing State	The Country issuing the travel document. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. 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 [ICAO_9303] 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 travel document holder 2.the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3.the digitized portraits (EF.DG2), 4.the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5.the other data according to LDS (EF.DG5 to EF.DG16). 6.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. [ICAO_9303]
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. [ICAO_9303] 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. [ICAO_9303]
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 [TR-03110-1]. 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.
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_9303], •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.
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 [ICAO_TR],. 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	A password needed for PACE authentication, e.g. CAN or MRZ.
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”
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 [TR-03110-1], (iv)writing the document details data, (v)writing the initial TSF data, (vi)signing the Document Security Object defined in [ICAO_9303] (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
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 traveller is applying for entry. [ICAO_9303]
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
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAO_9303]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
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 [ICAO_TR], namely (i) PACE or BAC and (ii) Passive Authentication with SOD. 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 PP 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 [ICAO_9303] (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 and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_9303], 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_P1]).
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 [TR-03110-1] 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_P1]). 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_P2]).
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. [ICAO_9303]
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.

5. ST INTRODUCTION

1 This section provides information about the TOE, which enables a potential user of the TOE to determine, whether the TOE implements the functionality required by the user.

5.1 ST Reference

Title:	JSAFE3_EPASS EAC Security Target Lite
Developer:	STMicroelectronics Z.I. Marcianise SUD I-81025 Marcianise (CE) ITALY
Status:	Final
Version:	Rev.A
Date:	13.March.2019

5.2 TOE Overview

2 The Security Target refers to the TOE JSAFE3_EPASS_EAC V1.0.0 a contact/contactless chip implementing the machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) [ICAO_9303] and implementing the advanced security methods, Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), Chip Authentication (CA) and the Active Authentication (AA) [ICAO_9303].

5.3 TOE Description

5.3.1 TOE Reference

JSAFE3_EPASS_EAC V1.0.0

5.3.2 TOE Definition

3 The Target of Evaluation (TOE) is a composite product comprising hardware and software The TOE is a contact/contactless chip and comprises the following elements:

- the STM IC ST31G480 Security Integrated Circuit with dedicated software and embedded cryptographic library. Rapport de manteinance ANSSI-CC-2016/58-M02, June 2017 [MntRep_ST31G480]
- the Java Card ™ Operating System JSAFE3 [JSAFE3_ST]
- the javacard applet JSAFE3_EPASS V.3.0.4 implementing the machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) programmed according to the Logical Data Structure (LDS) and implementing the advanced security methods, Extended Access Control (EAC), the Password Authenticated Connection Establishment (PACE), Chip Authentication (CA) and the Active Authentication (AA) as described in the 'ICAO Doc 9303' [ICAO_9303].
- the associated guidance documentation in printed copy delivered by courier and in .pdf format delivered crypted by e-mail:
  - JSAFE3-EPASS Operational User Guidance Rev. E 10 January 2019
  - JSAFE3-EPASS Preparative Procedure Rev. F 15 January 2019

4 The Target of Evaluation (TOE) is delivered at the end of Phase 2 Step 3 (see chap. 5.3.4) in wafer or micromodule D70, D76, CB6 format. The TOE is delivered by trusted courier.

5 The Figure 1 shows the composition of the TOE parts, including their location in the memory areas of the TOE. The TOE is a Java Card Flash memory based product.

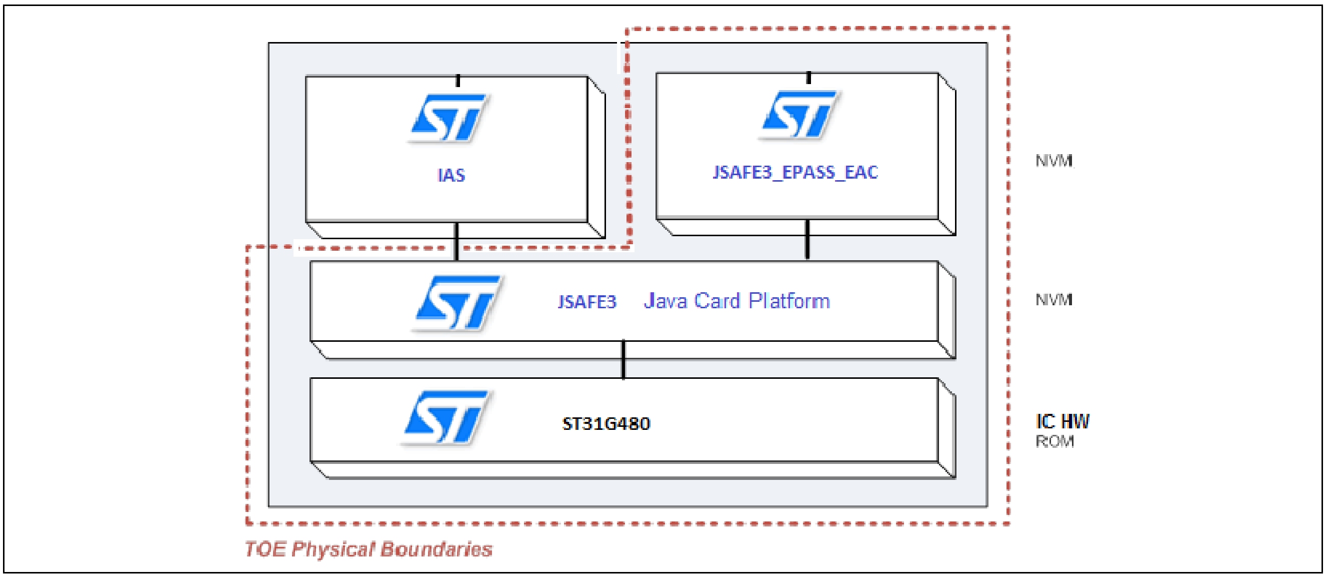


Figure 1 - TOE Overview

6 The ROM code holds the IC Dedicated Firmware belonging to the IC ST31G480

7 The Operating System JSAFE3 Java Card Platform and the JSAFE3_EPASS applet V.3.0.4 are located in the NVM.

8 During the Manufacturing phase the Java Card Package, including the JSAFE3_EPASS applet V.3.0.4 are loaded on the TOE.

9 The JSAFE3_EPASS applet V.3.0.4 is instantiated from this package during the initialisation of the TOE into the NVM memory area.

10 The JSAFE3_EPASS applet V.3.0.4 utilises the IC ST31G480 RAM and the NVM area for storage of operational and permanent data, in order to provide security functionality.

11 During operational use phase the JSAFE3_EPASS applet V.3.0.4 interacts with other external entities.

12 The Security Target of the underlying Operating System JSAFE3 Java Card Platform claims conformance to Java Card System – Closed Configuration Protection Profile, Version 3.0, December 2012 ([PP_JC_Closed])

13 This composite ST is based on the ST of the underlying Operating System JSAFE3 Java Card Platform [JSAFE3_ST].

14 **Important note**: The TOE is closed Java Card implementation with the applet JSAFE3_EPASS V.3.0.4 and the applet IAS V.2.0.3 installed and initialized as a single instances. The applet JSAFE3_EPASS V.3.0.4 is default selected after TOE reset. No post-issuance of further applets is possible to install on the TOE. The applets are installed and initialized in Phase 2, step 3. of TOE life cycle (see chap. 5.3.4).

5.3.3 TOE usage and security features for operational use

15 A State or Organization issues MRTDs to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST contains

- visual (eye readable) biographical data and portrait of the holder,
- a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
- data elements on the TOE according to LDS for contactless machine reading. The authentication of the traveller is based on
    i. the possession of a valid MRTD 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 MRTD.

16 The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

17 For this ST the MRTD is viewed as unit of:

- **the physical MRTD** as travel document in form of paper, plastic and chip (TOE). It presents visual readable data including (but not limited to) personal data of the MRTD holder
    i. the biographical data on the biographical data page of the MRTD,
    ii. the printed data in the Machine-Readable Zone (MRZ) and
    iii. the printed portrait.

- **the logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the MRTD holder
    i. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
    ii. the digitized portraits (EF.DG2),
    iii. the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) [1] or both
    iv. the other data according to LDS (EF.DG5 to EF.DG16) and
    v. the Document security object (SOD).

18 The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip (TOE) is uniquely identified by the Document Number.

19 The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the TOE) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO_9303]. These security measures include the binding of the MRTD's chip (TOE) to the passport book.

20 The logical MRTD 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 TOE.

[1] These biometric reference data are optional according to [ICAO_9303]. It is assumed that the issuing State or Organization uses this option and protects these data by means of EAC

21 The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the [ICAO_9303], and Password Authenticated Connection Establishment [ICAO_TR]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment

22 The TOE protects the integrity of logical MRTD by write-only-once access control and by physical means, and the confidentiality of logical MRTD by the Extended Access Control Mechanism.

23 The PACE is a security feature supported by the TOE. This mechanism shall be evaluated considering high attack potential (i.e. AVA_VAN.5). For the PACE protocol the TOE performs the following steps:

- The TOE 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.
- The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.
- The TOE and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
- 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 TOE provide private communication (secure messaging).

24 The TOE implement the Extended Access Control (EAC) as defined in [TR-03110-1]. The EAC consists of two parts

- (i) the Chip Authentication Protocol v.1 and
- (ii) the Terminal Authentication Protocol v.1

The Chip Authentication Protocol v.1

- (i) authenticates the TOE to the inspection system and
- (ii) establishes secure messaging which is used by Terminal Authentication Protocol 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 Protocol v.1 can only be performed if Chip Authentication Protocol v.1 has been successfully executed.

25 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.

26 The TOE implements the Active Authentication as defined in[ICAO_9303]. Keys for Active Authentication can be loaded into the TOE. These operations take place at personalization time

5.3.4 Life Cycle Phases Mapping

27 The life cycle of a MRTD is described in [PP-0056] and it is split in four phases.

Phase 1: “TOE Development”
Phase 2: “TOE Manufacturing”
Phase 3: “Personalization of the TOE MRTD application”
Phase 4: “TOE Operational Use”

In the beneath discussion, the following entities and roles are identified:
MRTD Embedded Software Developer: STMicroelectronics srl, Marcianise (CE) Italy
IC Developer: STMicroelectronics SAS, Rousset France
MRTD IC Manufacturer: STMicroelectronics srl, Marcianise (CE) Italy
MRTD Manufacturer: National accredited MRTD Manufacturing center (IPZS for Italy)
MRTD Personalization Agent: Public administration or National accredited MRTD personalization center enabled to issue personalized MRTD booklet (IPZS for Italy).

Life cycle phase 1: “TOE Development ”.

28 In this phase the TOE is developed.

29 This phase includes the following **Step 1**:

- Development of TOE *Embedded Software* performed by *MRTD Embedded Software Developer*:
  - Operating System JSAFE3 Java Card Platform
  - TOE MRTD application as Java card Applet
- TOE IC Development performed by *IC Developer*:
  - IC ST31G480 with its *Dedicated Software* and embedded cryptographic library
- TOE MRTD application guidance documentation

30 In the **Step 1** the *MRTD Embedded Software Developer* delivers the *Embedded Software* to the *IC Developer*. The *Embedded Software* is delivered in one of two possible configuration:

- **Embedded Software not Pre-Personalized**. No OS or JSAFE3 Java Card Platform or application code is delivered to *IC Developer*. Only pre-perso info to be used in “Pre-Personalization” process at *MRTD IC Manufacturer* premises are delivered. Pre-Perso info includes reference to keys for securing the download of flash code (OS, JSAFE3 Java Card platform and application) on the IC ST31G480.
- **Golden sample as full TOE image,** as output of phase 2 step 3 anticipated here.

31 **Step 2:** *IC Developer* loads on IC ST31G480 programmable memory the *Embedded Software* and alternatively do following :

- **Embedded Software not Pre-Personalized**. IC are securely delivered to the *MRTD IC Manufacturer*. The TOE life cycle restart from phase 2 step 3.
- **Golden sample as full TOE image.** The IC and the respective guidance documents are securely delivered to the *MRTD manufacturer*.
  The TOE life cycle restart from phase 2 step 4.

Life cycle phase 2: “TOE Manufacturing ”

32 This phase is split in the following steps:

- **Step 3:** The *MRTD IC manufacturer* receives IC loaded with *Dedicated Software* and with the *Embedded Software* not pre-personalized with the IC ST31G480 flash code loader secured with the key established as pre-perso info is Phase 1 step 1 and step2. *MRTD IC manufacturer* integrates applets JSAFE3_EPASS V.3.0.4 and IAS V.2.0.3 with JSAFE3 platform performing following steps:
  i. loading JSAFE3 Java Card Platform into IC ST31G480 programmable memory,
  ii. loading and instantiation of all applets
  iii. switch the JSAFE3 Java Card Platform in a secured closed state.
  iv. Dump the binary image of full components of TOE

  The IC with **full TOE image** is securely delivered to the *MRTD manufacturer*.

  The *MRTD IC manufacturer* delivers the guidance documentation to *MRTD manufacturer.*
- **Step 4:** The *MRTD manufacturer* combines the IC with hardware for the contactless interface in the passport booklet, equips MRTD’s chips with pre-personalization Data and eventually create the LDS structures as defined in [ICAO_9303].
- **Step 5:** The pre-personalized MRTD together with the IC Identifier is securely delivered from the *MRTD manufacturer* to the *MRTD Personalization Agent*. The *MRTD manufacturer* also provides the relevant parts of the guidance documentation to the *MRTD Personalization Agent.*

Life cycle phase 3: “Personalization of the TOE MRTD application”

33 The personalization of the MRTD includes the following actions in the **Step 6** performed by the *MRTD Personalization Agent*:

- the survey of the MRTD holder’s biographical data,
- the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- the printing of the visual readable data onto the physical MRTD,
- the writing of the TOE User Data and TSF Data into the logical MRTD. This step is performed by the Personalization Agent and includes but is not limited to creation of:
  i. the digital MRZ data (EF.DG1),
  ii. the digitized portrait (EF.DG2) and
  iii. the Document security object
- Configuration of the TSF if necessary.
- The signing of the Document security object by the Document Signer [ICAO_9303] finalizes the personalization of the genuine MRTD for the MRTD holder.
- The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use

34 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 Personalization Agent Authentication Key(s), the Terminal Authentication trust anchor, the effective date and the Chip Authentication Private Key

Life cycle phase 4: “TOE Operational Use ”

35 **Step 7**: The TOE is used as MRTD chip by the traveler and the inspection systems in the “TOE Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

36 **Application note:** The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify EF.DG16) in the Phase 4 “TOE Operational Use”. This will imply an update of the Document Security Object including the re-signing by the Document Signer.

37 **Application note**: The phases 1 and parts of phase 2 (Step 1, Step 2 and Step 3) are part of the TOE evaluation. The TOE delivery is after phase 2 Step 3. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation under ALC. The issuing State or Organization is responsible for these specific production steps.

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

38 The antenna and the applet IAS are not in the scope of the TOE.

39 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 MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

6. CONFORMANCE CLAIM

6.1 CC Conformance Claims

40 This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5. April 2017 ,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5. April 2017,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5. April 2017

as follows:

- Part 2 extended,
- Part 3 conformant.

41 Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5. April 2017 [CEM].

6.2 PP Claims

42 This ST claims strict conformance to the PPs:

- Protection Profile Machine Readable Travel Document with “ICAO Application", Extended Access Control with PACE Version 1.3.2, 05 December 2012 [PP-0056].

6.3 Package Claims

43 The evaluation of the TOE is a composite evaluation and uses the results of the CC evaluation provided by [JSAFE3_ST], [STLite_ST31G480] and [MntRep_ST31G480]. The TOE uses a certified J-SAFE3 Java Card Platform and IC ST31G480 by STMicroelectronics. J-SAFE3 Java Card Platform has been certified at assurance level EAL5+ its associated Security Target is [JSAFE3_ST]. The IC ST31G480 Secure Microcontroller with Cryptographic Library has been certified by ANSSI (ANSSI-CC-2017/61) with assurance level EAL5+: its associated Security Target Lite is [STLite_ST31G480] and the applicable Maintenance Report is [MntRep_ST31G480].

44 The evaluation assurance level of the TOE is EAL4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 as defined in [CC_P3] .

6.4 Conformance Rationale

45 This Security Target claims strict conformance to the protection profiles [PP-0056].

46 All sections of this Security Target regarding the **Security Problem Definition**, **Security Objectives Statement** and **Security Requirements Statement** for the TOE are taken over from [PP-0056].

47 This ST adds the following TOE Security Objective “**OT.Active_Auth_MRTD_Proof”,** the Security Objective for the Operational Environment “**OE.Active_Auth_Sign”, “OE.Active_Auth_Verif”,** the Organizational Security Policies “**P.Active_Auth”**

48 The operations done for the SFRs taken from [PP-0056] are clearly indicated.

49 This ST adds the following Security Functional Requirement **“FCS_COP.1/AA Cryptographic operation – Active Authentication”**

50 The **Security Assurance Requirements** statement for the TOE in this Security Target includes all the requirements for the TOE from [PP-0056].

7. SECURITY PROBLEM DEFINITION

7.1 Introduction

51 **Assets**

The assets to be protected by the TOE include the User Data stored in the TOE, user data transferred between the TOE and the terminal and MRTD tracing data

52 **User data stored on the TOE**

All data (being not authentication data) stored in the context of the ePassport application of the travel document as defined in [ICAO_TR] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_TR]).

This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [PP-0055].

Security property for the asset are: Confidentiality, Integrity and Authenticity.

53 **User data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)**

All data (being not authentication data) being transferred in the context of the ePassport application of the travel document as defined in [ICAO_TR] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO_TR]).

User data can be received and sent

Security property for the asset are: Confidentiality, Integrity and Authenticity.

54 **Travel Document tracing data**

Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PACE password.

TOE tracing data can be provided / gathered

Security property for the asset are: unavailability

55 **Logical travel document sensitive User Data**

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

56 **Authenticity of the travel document's chip**

The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.

57 **Accessibility to the TOE functions and data only for authorised subjects**

Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.

Security property for the asset are: availability

58 **Genuineness of the TOE**

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.This asset also covers 'Authenticity of the MRTD's chip' in [PP-0055].

Security property for the asset are: availability

59 **TOE internal secret cryptographic keys**

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality including Active Authentication Public Key in EF.DG15.

Security property for the asset are: Confidentiality and Integrity

60 **TOE internal non-secret cryptographic material**

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.

Security property for the asset are: Integrity and Authenticity

61 **Travel document communication establishment authorisation data**

Restricted-revealable19 authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.

Security property for the asset are: Confidentiality and Integrity

7.2 Subjects and external entities

62 This ST considers the following subjects:

63 **Travel Document Holder:** A person for whom the travel document Issuer has personalised the travel document. This entity is commensurate with 'MRTD Holder' in [PP-0055]. Please note that a travel document holder can also be an attacker.

64 **Travel Document Presenter (traveller):** A person presenting the travel document to a terminal and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [PP-0055]. Please note that a travel document presenter can also be an attacker.

65 **Terminal:** A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [PP-0055].

66 **Basic Inspection System with PACE (BIS-PACE):** A technical system being used by an inspecting authority 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). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication.

67 **Digital 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 [ICAO_9303]. This role is usually delegated to a Personalisation Agent.

68 **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 document 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. [ICAO_9303].

69 **Personalization 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:

- establishing the identity of the travel document holder for the biographic data in the travel document,
- enrolling the biometric reference data of the travel document holder,
- 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 [ICAO_9303],
- writing the document details data,
- writing the initial TSF data, (vi) signing the Document Security Object defined in [ICAO_9303] (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.

70 This entity is commensurate with 'Personalisation agent' in [PP-0055].

71 **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 cycle phase24. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [PP-0055].

72 **Country Verifying Certification Authority**

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in the form of Country Verifying CA Link-Certificates.

73 **Document Verifier**

The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the travel document in the limits provided by the issuing States or Organisations in the form of the Document Verifier Certificates

74 **Inspection system (IS):** A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.

75 The Extended Inspection System (EIS) performs the Advanced Inspection Procedure (Figure 2) and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both v.1 according to [TR-03110-1] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if

supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.

76 **Attacker**: A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained.The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE.This external entity is commensurate with 'Attacker' in [PP-0055].

Additionally to the previously definition an attacker is refined as followed: A threat agent trying

(i) to manipulate the logical travel document without authorization,

(ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4),

(iii) to forge a genuine travel document, or

(iv) to trace a travel document.

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

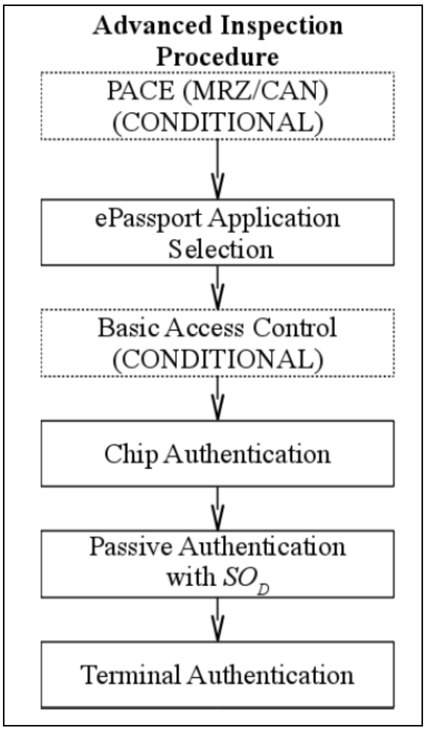

Advanced Inspection Procedure
PACE (MRZ/CAN) (CONDITIONAL)
ePassport Application Selection
Basic Access Control (CONDITIONAL)
Chip Authentication
Passive Authentication with SO_D
Terminal Authentication

Figure 2 – Advanced Inspection Procedure

7.3 Assumptions

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

79 **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 and/or BAC. 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 Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Justification:

The assumption A.Insp_Sys does not confine the security objectives of the [PP-0068] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

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

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

Justification:

This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [PP-0068] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol v.1.

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

The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the

Document Security Object contains only the hash values of genuine user data according to [ICAO_9303].

7.4 Threats

82 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.

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

- **Adverse action**: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip. The attack **T.Read_Sensitive_Data** is similar to the threat **T.Skimming** [PP-0055] in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.
- **Threat agent**: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document
- **Asset**: confidentiality of logical travel document sensitive user data (i.e. biometric reference)

84 **T.Counterfeit** **Counterfeit of travel document chip data**

- **Adverse action**: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document. The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.
- **Threat agent**: having high attack potential, being in possession of one or more legitimate travel documents
- **Asset**: authenticity of user data stored on the TOE

85 **T.Skimming Skimming travel document / Capturing Card-Terminal Communication**

- **Adverse action**: An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE
- **Threat agent**: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
- **Asset**: confidentiality of logical travel document data

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

Application Note: MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable cf. OE.Travel_Document_Holder.

86 **T.Eavesdropping Eavesdropping to the communication between TOE and inspection system**

- **Adverse action**: An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.
- **Threat agent**: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
- **Asset**: confidentiality of logical MRTD data

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

87 **T.Tracing Tracing travel document**

- **Adverse action**: An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE
- **Threat agent**: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.
- **Asset**: privacy of the travel document holder

Application Note: This Threat completely covers and extends “T.Chip-ID” from [PP-0055].

Application Note: A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this PP, see also the par. 1.2.5 above.

Application Note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document’s chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document) cannot be averted by the current TOE.

88 **T.Abuse-Func Abuse of Functionality**

- **Adverse action**: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.
- **Threat agent**: having high attack potential, being in possession of one or more legitimate travel documents
- **Asset**: integrity and authenticity of the travel document, availability of the functionality of the travel document

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

89 **T.Information_Leakage** **Information Leakage from MRTD's chip**

- **Adverse action**: An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.
- **Threat agent**: having high attack potential
- **Asset**: confidentiality of User Data and TSF-data of the travel document

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

90 **T.Phys-Tamper** **Physical Tampering**

- **Adverse action**: An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (i) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.
- **Threat agent**: having high attack potential, being in possession of one or more legitimate travel documents.
- **Asset**: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

Application Note: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g.authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

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

- **Adverse action**: An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.
- **Threat agent**: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation.
- **Asset**: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document.

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

92 **T.Forgery** **Forgery of data on MRTD's chip**

- **Adverse action**: An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.
- **Threat agent**: having high attack potential.
- **Asset**: integrity of the travel document.

7.5 Organizational Security Policies

93 The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see [CC_P1]).

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

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication v.1.

95 **P.Personalisation** **Personalisation of the travel document by issuing State or Organisation only**

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

96 **P.Pre-Operational** **Pre-operational handling of the travel document**

i. The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.

ii. The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE

iii. The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase.

iv. If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

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

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

1. The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA).
2. The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer
3. A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

98 **P.Trustworthy_PKI** **Trustworthiness of PKI**

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (Document Signer) and Document Signers shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

99 **P.Manufact** **Manufacturing of the travel document's chip**

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

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

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

1. The related terminals (basic inspection system) shall be used by terminal operators and by travel document holders as defined in [ICAO_9303].
2. They shall implement the terminal parts of the PACE protocol, of the Passive Authentication and use them in this order. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3. The related terminals need not to use any own credentials.
4. They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document).
5. The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

101 **P.Active_Auth** **Active Authentication**

The TOE implements the Active Authentication according to [ICAO_9303]

8. SECURITY OBJECTIVES

102 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.

8.1 Security Objectives for the TOE

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

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

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

105 **OT.Chip_Auth_Proof** **Proof of the travel document's chip authenticity**

The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Protocol v1. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application note: The OT.Chip_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 Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO_9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

106 **OT.Data_Integrity** **Integrity of Data**

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

107 **OT.Data_Authenticity** **Authenticity of Data**

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side.The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the

PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE).

108 **OT.Data_Confidentiality** **Confidentiality of data**

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

109 **OT.Tracing** **Tracing travel document**

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

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

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

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

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document:

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

Application note: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

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

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD’s chip Embedded Software. This includes protection against attacks with enhanced-basic attack potential by means of:

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

- reverse engineering to understand the design and its properties and functions.

113 **OT.AC_Pers** **Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application note: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

114 **OT.Prot_Malfunction** **Protection against Malfunctions**

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

115 **OT.Identification** **Identification and Authentication of the TOE**

The TOE must provide means to store Initialisation and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

116 **OT.Active_Auth_MRTD_Proof** **Proof of MRTD’s chip authenticity by Active Authentication**

The TOE shall support the Inspection Systems to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in ‘ICAO Doc 9303’ [ICAO_9303]. The Active Authentication mechanism provided by the TOE shall resist to high potential attack.

8.2 Security Objectives for the Operational Environment

Issuing State or Organization

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

118 **OE.Legislative_Compliance** **Issuing of the travel document**

The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

119 **OE.Passive_Auth_Sign** **Authentication of travel document by Signature**

The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained.A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO_9303]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO_9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document..

120 **OE.Personalization** **Personalization of travel document**

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO_9303], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO_9303] (in the role of a DS).

121 **OE.Auth_Key_Travel_Document** **Travel document Authentication Key**

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

Justification: This security objective for the operational environment is needed in order to counter the Threat **T.Counterfeit** as it specifies the pre-requisite for the Chip Authentication Protocol v.1 which is a features of the TOE.

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

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

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

123 **OE.Active_Auth_Sign Active Authentication of logical MRTD by Signature**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRTD's Active Authentication Private Key, 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 MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

Receiving State or Organization

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

124 **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 traveller 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 and/or the Basic Access Control. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol v.1 to verify the Authenticity of the presented travel document's chip.

Justification: This security objective for the operational environment is needed in order to handle the Threat **T.Counterfeit** and the Assumption **A.Insp_Sys** by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document counters **T.Forgery** and **A.Passive_Auth**. This is done because a new type of Inspection System is introduced in this ST as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

125 **OE.Prot_Logical_Travel_Document Protection of data from the logical travel document**

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol v.1.

Justification: This security objective for the operational environment is needed in order to handle the Assumption **A.Insp_Sys** by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1

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

The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Justification: This security objective for the operational environment is needed in order to handle the Threat **T.Read_Sensitive_Data**, the Organisational Security Policy

P.Sensitive_Data and the Assumption **A.Auth_PKI** as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

127 **OE.Terminal** **Terminal operating**

The terminal operators must operate their terminals as follows:

- The related terminals (basic inspection systems) are used by terminal operators and by travel document holders as defined in [ICAO_9303].
- The related terminals implement the terminal parts of the PACE protocol, of the Passive Authentication (by verification of the signature of the Document Security Object) and use them in this order. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
- The related terminals need not to use any own credentials.
- The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO_9303]).
- The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE.

Application note: OE.Terminal completely covers and extends “OE.Exam_MRTD”, “OE.Passive_Auth_Verif“ and “OE.Prot_Logical_MRTD” from [PP-0055].

128 **OE.Travel_Document_Holder** **Travel document holder Obligations**

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

129 **OE.Active_Auth_Verif** **Verification by Active Authentication**

The inspection systems to check the MRTD authenticity may use the active authenticatio verification, this is a stronger mechanism to guaranty the authenticity of the MRTD.

8.3 Security Objective Rationale

130 The following table provides an overview for security objectives coverage.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Active_Auth_MRTD_Proof	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_travel_Docum.	OE.Ext_Insp_Systems	OE.Personalization	OE.Passive_Auth_Verif	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Read_Sensitive_Data	X														X			X							
T.Counterfeit		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.Personalization			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					
P.Active_Auth													X											X	X
A.Insp_Sys																X	X								
A.Auth_PKI															X			X							
A.Passive_Auth																X				X					

Table 1: Security Objectives Rationale

131 The OSP P.Personalisation “Personalisation of the travel document by issuing State or Organisation only” addresses the (i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment OE.Personalisation “Personalisation of logical travel document”, and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers “Access Control for Personalisation of logical travel document”. Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to OT.Identification “Identification and Authentication of the TOE”. The security objective OT.AC_Pers limits the management of TSF data and the management of TSF to the Personalisation Agent.

132 The OSP P.Sensitive_Data “Privacy of sensitive biometric reference data” is fulfilled and the threat T.Read_Sensitive_Data “Read the sensitive biometric reference data” is countered by the TOE-objective OT.Sens_Data_Conf “Confidentiality of sensitive biometric reference data” requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data’s

confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by OE.Authoriz_Sens_Data “Authorization for use of sensitive biometric reference data”. The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems “Authorization of Extended Inspection Systems”.

133 The OSP P.Terminal “Abilities and trustworthiness of terminals” is countered by the security objective OE.Exam_Travel_Document additionally to the security objectives from PACE PP [PP-0068]. OE.Exam_Travel_Document enforces the terminals to perform the terminal part of the PACE protocol.

134 The OSP P.Active_Auth “Active Authentication” addresses the active authentication protocol as described in [ICAO_9303]. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Active_Auth_Sign “Active Authentication of logical MRTD by Signature” and verified by the inspection system according to OE.Active_Auth_Verif “Verification by Active Authentication”. This is possible only because genuine TOE enforce Active Authentication as specified in OT.Active_Auth_Proof.

135 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 an identification and authenticity proof required by OT.Chip_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”. 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 v.1 to verify the authenticity of the travel document’s chip.

136 The threat T.Forgery “Forgery of data” addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. Additionally to the security objectives from PACE PP [PP-0068] which counter this threat, the examination of the presented MRTD passport book according to OE.Exam_Travel_Document “Examination of the physical part of the travel document” shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

137 OT.Active_Auth_MRTD_Proof “Proof of MRTD’s chip authenticity by Active Authentication” using a authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15 The TOE environment will also detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Active_Auth_Sign “Active Authentication of logical MRTD by Signature” and verified by the inspection system according to OE.Active_Auth_Verif “Verification by Active Authentication”.

138 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, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol v.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.

139 The assumption A.Passive_Auth “PKI for Passive Authentication” is directly covered by the security objective for the TOE environment OE.Passive_Auth_Sign “Authentication of travel document by Signature” from PACE PP [PP-0068] covering the necessary

procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_Travel_Document “Examination of the physical part of the travel document”.

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

9. EXTENDED COMPONENTS DEFINITION

141 This Security Target uses components defined as extensions to [CC_P2]. All these extended components are derived from [PP-0056].

9.1 Definition of the Family FAU_SAS Audit Data Storage

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

143 The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling

FAU_SAS Audit Data Storage
1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: authorized users] with the capability to store [assignment: list of audit information] in the audit records.

9.2 Definition of the Family FCS_RND Generation of random numbers

144 To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

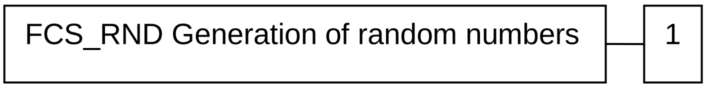
145 The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behaviour:

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:



FCS_RND.1 Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

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 [assignment*: a defined quality metric*].

9.3 Definition of the Family FMT_LIM Limited capabilities and availability

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

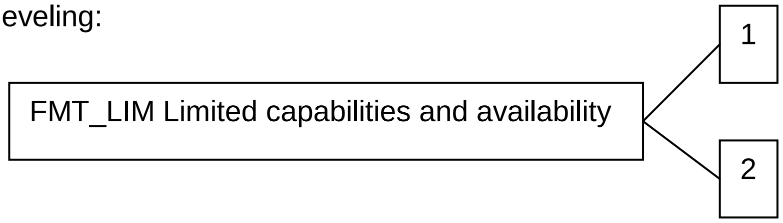
147 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour:

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:



FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) which are necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

148 To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

149 The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

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

150 The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

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

Application Note:

The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

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

or conversely,

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

The combination of both requirements shall enforce the policy.

9.4 Definition of the Family FPT_EMS TOE Emanation

151 The sensitive family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of [CC_P2].

152 The family "TOE Emanation (FPT_EMS)" is specified as follows.

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

9.5 Definition of the Family FIA_API

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

154 **Application note**: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 ([CC_P2], chapter "Explicitly stated IT security requirements (APE_SRE)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behavior:

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:

FIA_API Authentication Proof of Identity
1

FIA_API.1Authentication Proof of Identity

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].

10. SECURITY REQUIREMENTS

10.1 Overview

155 This part of the PP defines the detailed security requirements that shall be satisfied by the TOE. The statement of **TOE security requirements** shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

156 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in section 8.1 of Part 1 of the Common Criteria [CC_P1]Each of these operations is used in this ST.

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

158 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *slanted and underlined*.

159 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *slanted and underlined*.

160 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.

161 This part defines the detailed security requirements that are satisfied by the TOE. These requirements comprise functional components from CC Part 2 [CC_P1]Extended components as defined in Chapter 9, and the assurance components as defined for the Evaluation Assurance Level EAL4 from CC Part 3 [CC_P1] augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

162 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 7. Note, that all these subjects are acting for homonymous external entities. 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:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorization after start-up)
	CVCA	roles defined in the certificate used for authentication ([TR-03110-1]); 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

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

Table 2: Definition of security attributes

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	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the
Public Key (PK_{CVCA})	Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR-03110-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection

Name	Data
	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 [11].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication v.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.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organization with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol v.1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

Table 3: Definition of security attributes

Application note: 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.

163 The following table summarizes all TOE security functional requirements of this ST:

Class FAU: Security Audit	
FAU_SAS.1	Audit Storage
Class FCS: Cryptographic Support	
FCS_CKM.1/CA-DH-3DES	Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys
FCS_CKM.1/CA-DH-AES	
FCS_CKM.1/CA-ECDH-3DES	
FCS_CKM.1/CA-ECDH-AES	
FCS_CKM.1/DH-PACE-3DES	Cryptographic key generation – Diffie-Hellman for PACE session keys
FCS_CKM.1/DH-PACE-AES	
FCS_CKM.1/ECDH-PACE-3DES	
FCS_CKM.1/ECDH-PACE-AES	
FCS_CKM.4	Cryptographic key destruction – Session key
FCS_COP.1/PACE_ENC	Cryptographic operation – Encryption/Decryption AES/3DES
FCS_COP.1/PACE_MAC	Cryptographic operation – MAC
FCS_COP.1/CA_ENC	Cryptographic operation – Symmetric Encryption/Decryption
FCS_COP.1/CA_MAC	Cryptographic operation – MAC
FCS_COP.1/SIG_VER	Cryptographic operation - Signature verification by travel document
FCS_COP.1/AA	Cryptographic operation – Active Authentication
FCS_RND.1	Random number generation - Quality metric for random numbers
Class FIA: Identification and Authentication	
FIA_AFL.1/PACE	Authentication failure handling - PACE authentication using non-blocking authorisation data
FIA_UID.1/PACE	Timing of identification
FIA_UAU.1/PACE	Timing of authentication
FIA_UAU.4/PACE	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5/PACE	Multiple authentication mechanisms
FIA_UAU.6/PACE	Re-authenticating of the Terminal by the TOE
FIA_UAU.6/EAC	Re-authenticating of the Terminal by the TOE
FIA_API.1	Authentication Proof of Identity
Class FDP: User Data Protection	
FDP_RIP.1	Subset residual information protection
FDP_UCT.1/TRM	Basic data exchange confidentiality - MRTD
FDP_UIT.1/TRM	Data exchange integrity
FDP_ACC.1/TRM	Subset access control
FDP_ACF.1/TRM	Security attribute based access control
Class FMT: Security Management	
FMT_SMF.1	Specification of management functions
FMT_SMR.1/PACE	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data - Writing of Initialization Data and Pre-personalization Data
FMT_MTD.1/INI_DIS	Management of TSF data - Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/PA	Management of TSF data - Personalization Agent
FMT_MTD.1/CVCA_INI	Management of TSF data - Initialization of CVCA Certificate and Current Date
FMT_MTD.1/CVCA_UPD	Management of TSF data - Country Verifying Certification Authority
FMT_MTD.1/DATE	Management of TSF data – Current Date
FMT_MTD.1/CAPK	Management of TSF data – Chip Authentication Private Key

FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
FMT_MTD.3	Secure TSF data
Class FTP: Trusted Path/Channels	
FTP_ITC.1/PACE	Inter-TSF trusted channel after PACE
Class FPT: Protection of the TSF	
FPT_EMS.1	TOE emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack

Table 4: SFR Overview

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

10.2 Class FAU Security Audit

165 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[2] with the capability to store the Identification and Pre-Personalization Data[3] in the audit records.

166 **Application note** : The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS).

10.3 Class Cryptographic Support (FCS)

167 The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below ([CC_P2]). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

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

[2] [assignment: *authorized users*]

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[*assignment*: cryptographic key generation algorithm]* and specified cryptographic key sizes *[*assignment*: cryptographic key sizes]* that meet the following:[selection: *based on the Diffie-Hellman key derivation protocol compliant to [TR-03110-1] and [PKCS_#3], based on an ECDH protocol compliant to [TR-03111]*][4].

Iteration	[Assignment: Cryptographic key generation algorithm]	[Assignment: Cryptographic key sizes]	[Selection: Based on……….]
/CA-DH-3DES	*DH Key Agreement Algorithm*	*112 bits*	*Diffie-Hellman key derivation protocol compliant to [TR-03110-1] and [PKCS_#3]*
/CA-DH-AES	*DH Key Agreement Algorithm*	*128, 192 and 256 bits*	*Diffie-Hellman key derivation protocol compliant to [TR-03110-1] and [PKCS_#3]*
/CA-ECDH-3DES	*ECDH Key Agreement Algorithm*	*112 bits*	*based on an ECDH protocol compliant to [TR-03111]*]
/CA-ECDH-AES	*ECDH Key Agreement Algorithm*	*128, 192 and 256 bits*	*based on an ECDH protocol compliant to [TR-03111]*]

168 **Application note**: For [PKCS_#3] the RSA key length supported are 1024 and 2048 bits anf for [TR-03111] the EC key length supported are 160, 192, 224, 256, 320, 384, 512 and 521 bits.

169 **Application note:** The TOE implements the hash functions 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. The TOE implements additional hash functions SHA-224, SHA-256, SHA 384 and SHA 512.

170 **Application note:** The TOE destroys any session keys in accordance with FCS_CKM.4

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]
fulfilled by FCS_CKM.2/DH.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[selection: Diffie-Hellman-Protocol compliant to [PKCS_#3], ECDH compliant to [TR-03111]]*[5] and specified cryptographic key sizes *[assignment: cryptographic key sizes]* that meet the following: [ICAO_TR][6].

[4] [assignment: list of standards]

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

[6] [assignment: list of standards]

Iteration	[Selection: ………….]	[Assignment: Cryptographic key sizes]
/DH-PACE-3DES	*Diffie-Hellman-Protocol compliant to [PKCS_#3]*	*112 bits*
/DH-PACE-AES	*Diffie-Hellman-Protocol compliant to [PKCS_#3]*	*128, 192 and 256 bits*
/ECDH-PACE-3DES	*ECDH compliant to [TR-03111]*	*112 bits*
/ECDH-PACE-AES	*ECDH compliant to [TR-03111]*	*128, 192 and 256 bits*

171 **Application note:** For [PKCS_#3] the RSA key length supported are 1024 and 2048 bits anf for [TR-03111] the EC key length supported are 160, 192, 224, 256, 320, 384, 512 and 521 bits.

172 **Application note:** The TOE generates a shared secret value K with the terminal during the PACE protocol. This protocol may be based on the Diffie-Hellman-Protocol compliant to [PKCS_#3],] or on the ECDH compliant to [TR-03111]]. 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_TR] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

173 **Application note:** The TOE supports the following standardized elliptic curve and RSA key:

1024-bit MODP Group with 160-bit Prime Order Subgroup
2048-bit MODP Group with 224-bit Prime Order Subgroup
2048-bit MODP Group with 256-bit Prime Order Subgroup
NIST P-192 (secp192r1), NIST P-224 (secp224r1), NIST P-256 (secp256r1), NIST P-384 (secp384r1), NIST P-521 (secp521r1)
BrainpoolP192r1, BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1

FCS_CKM.4 Cryptographic key destruction – Session Key

Hierarchical to: No other components

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physical deletion by overwriting the memory data with zeros*[7] that meets the following: *none*[8].

10.4 Cryptographic operation (FCS_COP.1)

174 The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below ([CC_P2]). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

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

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

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

FCS_COP.1.1/PACE_ENC The TSF shall perform secure messaging – encryption and decryption[9] in accordance with a specified cryptographic algorithm *AES and 3DES* in CBC mode[10] and cryptographic key sizes *112, 128, 192 and 256* bit[11] that meet the following: compliant to [ICAO_TR][12].

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[13] in accordance with a specified cryptographic algorithm *CMAC and Retail-MAC*[14] and cryptographic key sizes *112, 128, 192 and 256* bit[15] that meet the following: compliant to [ICAO_TR][16].

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[17] in accordance with a specified cryptographic algorithm *AES and 3DES*[18] and cryptographic key sizes *112, 128, 192 and 256* bit[19] that meet the following: *compliant to [TR-03110-1]*[20].

[9] [assignment: *list of cryptographic operations*]
[10] [assignment: *cryptographic algorithm*]
[11] [assignment: *cryptographic key sizes*]
[12] [assignment: *list of standards*]
[13] [assignment: *list of cryptographic operations*]
[14] [assignment: *cryptographic algorithm*]
[15] [assignment: *cryptographic key sizes*]
[16] [assignment: *list of standards*]
[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]

175 **Application note:** The TOE implements the cryptographic primitives (e.g. 3DES 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 v.1.

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[21] in accordance with a specified cryptographic algorithm *CMAC and Retail-MAC* [22] and cryptographic key sizes *112, 128, 192 and 256* bit[23] that meet the following: *compliant to [TR-03110-1]*[24].

176 **Application note:** The TOE implements 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 v.1.

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
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[25] in accordance with a specified cryptographic algorithm *ECDSA, RSA PSS and RSA PKCS#1*[26] and cryptographic key sizes *192, 224, 256, 320, 384, 512, and 521 bits for EC Key and 1024 and 2048 bits for RSA key* that meet the following: *[TR-03111], [RFC3447] and [PKCS1_v1_5]*[27].

177 **Application note:** The TOE implements signature algorithms to implemented the Terminal Authentication Protocol v.1. The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

FCS_COP.1/AA Cryptographic operation – Active Authentication

Hierarchical to: No other components.

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

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]
[25] [assignment: *list of cryptographic operations*]
[26] [assignment: *cryptographic algorithm*]
[27] [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]:fulfilled by **FMT_MTD.1/KEY_WRITE**
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AA The TSF shall perform *Table 5 column 1*[28] in accordance with a specified cryptographic algorithm *Table 5 column 2*[29] and cryptographic key sizes *Table 5 column 3*[30] that meet the following standards *Table 5 column 4*[31].

list of cryptographic operations	***cryptographic algorithm***	***cryptographic key sizes***	***list of standards***
digital signature creation	*RSA CRT*	*1024 and 2048 bits*	[ISO_9796-2]
digital signature creation	*ECDSA*	*192,224,256,320,384,512 and 521 bits*	*[TR-03111]*

Table 5: FCS_COP.1/AA

10.5 Random Number Generation (FCS_RND.1)

178 The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below ([CC_P2]).

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 *DRG.3 capabilities defined in [AIS31/20] standard*[32].

179 **Application note:** TOE to generate random numbers (random nonce) used for the authentication protocol (PACE).

10.6 Class FIA Identification and Authentication

180 **Application note:** The Table 7 provides an overview on the authentication mechanisms used.

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

Table 6: Overview on the authentication mechanisms

[28] [assignment: *list of cryptographic operations*]
[29] [assignment: *cryptographic algorithm*]
[30] [assignment: *cryptographic key sizes*]
[31] [assignment: *list of standards*]
[32] [assignment: *positive integer number*]

181 Note the Chip Authentication Protocol v.1 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 v.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.

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: fulfilled by FIA_UAU.1/PACE

FIA_AFL.1.1/PACE The TSF shall detect when *1*[33] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password

FIA_AFL.1.2/PACE When the defined number of unsuccessful authentication attempts has been met[34], the TSF shall *consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords*[35].

182 The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below ([CC_P2]).

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_TR] ,
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-03110-1]
5. to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-1]
6. *Personalization agent authentication by authentication key*[36].

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.

183 **Application note:** 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

[33] [assignment: *a defined quality metric*]
[34] [selection: *met, surpassed*]
[35] [assignment: *list of actions*]
[36] [assignment: *list of TSF-mediated actions*]

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 v.1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol v.1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

184 **Application note:** 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).

185 **Application note:** 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).

186 The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below ([CC_P2]).

FIA_UAU.1/PACE Timing of authentication

Hierarchical to: No other components.

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

FIA_UAU.1.1/PACE The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO_TR] ,
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-03110-1]
6. to carry out the Terminal Authentication Protocol v.1 according to [TR-03110-1]
7. *none*[37]

FIA_UAU.1.1/PACE The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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

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

188 The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below ([CC_P2]).

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_TR],
2. Authentication Mechanism based on *AES*[38].
3. Terminal Authentication Protocol v.1 according to [TR-03110-1]

189 **Application note:** 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.

190 The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below ([CC_P2]).

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_TR],
2. Passive Authentication according to [ICAO_9303]
3. Secure messaging in MAC-ENC mode according to [ICAO_TR] ,
4. Symmetric Authentication Mechanism based on *AES*[39].
5. Terminal Authentication Protocol v.1 according to [TR-03110-1]

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 *Symmetric Authentication Mechanism with Personalisation Agent Key(s)* .
3. After run of the Chip Authentication Protocol v.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*[40]

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

[39] [assignment: *list of multiple authentication mechanisms]*

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

191 The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below ([CC_P2]).

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 conditions each command sent to the TOE after successful run of the PAC E protocol shall be verified as being sent by the PACE terminal[41].

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1/EAC The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol v.1 shall be verified as being sent by the Inspection System[42].

193 **Application note:** The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO_9303] 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.

194 The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below ([CC_P2]).

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a Chip Authentication Protocol v.1 according to [ICAO_TR][43] to prove the identity of the TOE[44].

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

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

[43] [assignment: *authentication mechanism*]

[44] [assignment: *authentication role*]

195 **Application note:** This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [ICAO_TR]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO_9303]. 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).

10.7 Class FDP User Data Protection

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* 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 [ICAO_TR]) [45]
3. *None*[46].

196 The TOE shall meet the requirement "Subset access control (FDP_UCT.1)" as specified below ([CC_P2]).

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] fulfilled by FTP_ITC.1/PACE
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
fulfilled by FDP_ACC.1/TRM

FDP_UCT.1.1/TRM The TSF shall enforce the Access Control SFP[47] to be able to transmit and receive[48] user data in a manner protected from unauthorised disclosure.

197 The TOE shall meet the requirement "Subset access control (FDP_UIT.1)" as specified below ([CC_P2]).

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

[45] [assignment: *list of objects*]
[46] [assignment: *list of objects*]
[47] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[48] [selection: *transmit receive*]

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[49] to be able to transmit and receive[50] user data in a manner protected from modification, deletion, insertion and replay[51] errors.

FDP_UIT.1.2/TRM The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[52] has occurred.

198 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below ([CC_P2]).

FDP_ACC.1/TRM Subset access control

Hierarchical to: No other components.

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

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP[53] on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document[54].

199 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below ([CC_P2]).

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: fulfilled by FDP_ACC.1/TRM

FDP_ACF.1.1/TRM The TSF shall enforce the Access Control SFP[55] 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[56]
3. Security attributes
   a. PACE Authentication
   b. Terminal Authentication v.1
   c. Authorisation of the Terminal[57].

[49] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[50] [selection: *transmit receive*]
[51] [selection: *modification, deletion, insertion, replay*]
[52] [selection: *modification, deletion, insertion, replay*]
[53] [assignment: *access control SFP*]
[54] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[55] [assignment: *access control SFP*]
[56] e.g. Chip Authentication v.1 and ephemeral keys

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_TR] after a successful PACE authentication as required by FIA_UAU.1/PACE[58].

FDP_ACF.1.3/TRM The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[59].

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[60].

200 **Application note:** The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [TR-03110-1]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (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.

201 **Application note:** Please note that the Document Security Object (SOD) stored in EF.SOD ([ICAO_9303]) 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, ([ICAO_TR]).

202 **Application note:** 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 v.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).

10.8 Class FMT Security Management

203 **Application note**: The SFR FMT_SMF.1 and FMT_SMR.1/PACE provide basic requirements to the management of the TSF data.

204 The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below ([CC_P2]).

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

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

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

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

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. Initialization,
2. Pre-personalization,
3. Personalization,
4. Configuration[61].

205 The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below ([CC_P2]).

FMT_SMR.1/PACE Security roles

Hierarchical to: No other components.

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

FMT_SMR.1.1/PACE The TSF shall maintain the roles

1. Manufacturer ,
2. Personalisation Agent,
3. Terminal,
4. PACE authenticated BIS-PACE,
5. Country Verifying Certification Authority,
6. Document Verifier,
7. Domestic Extended Inspection System
8. Foreign Extended Inspection System[62].

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

206 **Application note**: 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.

207 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below ([CC_P2]).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability: fulfilled by FMT_LIM.2

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow

1. User Data to be manipulated and disclosed
2. TSF data to be manipulated or disclosed
3. software to be reconstructed
4. substantial information about construction of TSF to be gathered which may enable other attacks and

[61] [assignment: *list of management functions to be provided by the TSF*]
[62] [assignment: *the authorized identified roles*]

5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed*[63].

208 The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below ([CC_P2]).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow

1. User Data to be manipulated and disclosed
2. TSF data to be manipulated or disclosed
3. software to be reconstructed
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed*[64].

209 **Application note:** The formulation of “Deploying Test Features …” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

210 **Application note:** 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.

211 The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below ([CC_P2]). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

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

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write[65] the Initialization Data and Pre-personalization Data[66] to the Manufacturer[67].

212 **Application note:** The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

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

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

[65] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]

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

[67] [assignment: *the authorized identified roles*]

Hierarchical to: No other components.

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

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to read out[68] Initialization Data and Pre-personalization Data[69] to the Personalization Agent[70].

213 **Application note:** 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

FMT_MTD.1.1/PA The TSF shall restrict the ability to write[71] the Document Security Object (SOD)[72] to the Personalization Agent [73].

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

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write[74] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date,
4. *None* [75]

to the *Personalization Agent* [76].

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

Hierarchical to: No other components.

[68] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[69] [assignment: *list of TSF data*]
[70] [assignment: *the authorized identified roles*]
[71] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[72] [assignment: *list of TSF data*]
[73] [assignment: *the authorized identified roles*]
[74] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[75] [assignment: *list of TSF data*]
[76] [assignment: *the authorized identified roles*]

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

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update[77] the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate,
to Country Verifying Certification Authority [78].

215 **Application note:** The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates ([TR-03110-1]). 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-03110-1]).

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify[79] the Current Date[80] to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. Domestic Extended Inspection System[81].

216 **Application note:** The authorized roles are identified in their certificate ([TR-03110-1]) 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-03110-1]).

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

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *load*[82] the Chip Authentication Private Key[83] to the *Personalization Agent* [84].

217 **Application note:** 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/AA Management of TSF data – Active Authentication Private Key

Hierarchical to: No other components.

[77] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[78] [assignment: *the authorized identified roles*]
[79] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[80] [assignment: *list of TSF data*]
[81] [assignment: *the authorized identified roles*]
[82] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[83] [assignment: *list of TSF data*]
[84] [assignment: *the authorized identified roles*]

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

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *load*[85] the *Active Authentication Private Key*[86] to the *Personalization Agent* [87].

218 **Application note:** The verb "load" means here that the Active Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[88] the

1. PACE passwords ,
2. Chip Authentication Private Key,
3. *Active Authentication Private Key*
4. Personalisation Agent Keys[89]

to none[90].

219 The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below ([CC_P2]):

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data: fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD

FMT_MTD.3.1 The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[91].

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

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

[85] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[86] [assignment: *list of TSF data*]
[87] [assignment: *the authorized identified roles*]
[88] [selection: *change, default, query, modify, delete, clear*, [assignment: *other operations*]]
[89] [assignment: *list of TSF data*]
[90] [assignment: *the authorized identified roles*]
[91] [assignment: *list of TSF data*]

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.**

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.

221 **Application note:** The Terminal Authentication v.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.

10.9 Class FTP Trusted Path/Channels

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

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FTP_ITC.1.1/PACE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE	The TSF shall enforce communication via the trusted channel for any data exchange between the TOE and the Terminal[92].

222 **Application note:** The TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

223 **Application note:** 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.

10.10 Class FPT Protection of the Security Functions

224 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

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

bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

225 The TOE shall meet the requirement "TOE Emanation (FPT_EMS.1)" as specified below ([CC_P2]).

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_EMS.1.1 The TOE shall not emit *power variations, timing variations during command execution*[93] in excess of *non-useful information*[94] enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K MAC, PACE-KEnc),
3. the ephemeral private key ephem SK PICC-PACE,
4. *none,*
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key
7. *Active Authentication Private Key* [95] and
8. *none.*

FPT_EMS.1.2 The TSF shall ensure any users[96] are unable to use the following interface smart card circuit contacts[97] to gain access

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K MAC, PACE-KEnc),
3. the ephemeral private key ephem SK PICC-PACE,
4. *none,*
5. Personalisation Agent Key(s),
6. Chip Authentication Private Key
7. *Active Authentication Private Key* [98] and
8. *none.*

226 **Application note**: 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 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.

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

228 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below ([CC_P2]).

[93] [assignment: *types of emissions*]
[94] [assignment: *specified limits*]
[95] [assignment: *list of types of TSF data*]
[96] [assignment: *type of users*]
[97] [assignment: *type of connection*]
[98] [assignment: *list of types of TSF data*]

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to operating conditions causing a TOE malfunction,
2. failure detected by TSF according to FPT_TST.1[99].
3. *none*

229 The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below ([CC_P2]).

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 before calling a security sensitive module*[100] to demonstrate the correct operation of the TSF[101].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data[102].

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

230 **Application note**: If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

231 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below ([CC_P2]).

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[103] to the TSF[104] by responding automatically such that the SFRs are always enforced.

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

[100] [selection: *during initial start-up.. [assignment: conditions under which self test should occur*]

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

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

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

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

232 **Application note**: 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.

10.11 Security Assurance Requirements for the TOE

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

234 Evaluation Assurance Level 4 (EAL4) and augmented by the following component:

- AVA_VAN.5 (Advanced methodical vulnerability analysis).
- ALC_DVS.2 (Sufficiency of security measures)
- ATE_DPT.2 (Testing: security enforcing modules)

The following table lists the applicable assurance components

ASSURANCE CLASS	ASSURANCE COMPONENTS
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.2 Sufficiency of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures These SARs ensure proper installation and configuration: the TOE will be properly configured and the TSFs are configured to process as expected
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.2 Testing: security enforcing modules

	ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample.
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 7: Assurance Requirements - EAL 4 extended with ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5

10.12 Security Requirements Rationale

10.12.1 Security Functional Requirements Rationale

235 The following table provides an overview for security objectives coverage.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_MRTD_Proof
FAU_SAS.1			x				x						
FCS_CKM.1/DH-PACE-3DES				x	x	x							
FCS_CKM.1/DH-PACE-AES				x	x	x							
FCS_CKM.1/ECDH-PACE-3DES				x	x	x							
FCS_CKM.1/ECDH-PACE-AES				x	x	x							
FCS_CKM.1/CA-DH-3DES	x	x	x	x	x	x							
FCS_CKM.1/CA-DH-AES	x	x	x	x	x	x							
FCS_CKM.1/CA-ECDH-3DES	x	x	x	x	x	x							
FCS_CKM.1/CA-ECDH-AES	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		x											
FDP_ACC.1/TRM	x		x	x		x							
FDP_ACF.1/TRM	x		x	x		x							
FDP_RIP.1				x	x	x							
FDP_UCT.1/TRM	x			x		x							
FDP_UIT.1/TRM				x		x							
FMT_SMF.1		x	x	x	x	x	x						
FMT_SMR.1/PACE		x	x	x	x	x	x						

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_MRTD_Proof
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/AA	x	x		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			

Table 8: Coverage of Security Objectives for the TOE by SFR

10.12.2 Rationale for the Fulfilment of the Security Objectives for the TOE

236 In the following, a detailed justification as required to show the suitability and sufficiency of the security functional requirements to achieve the security objectives defined for the TOE is given.

OT.Identification

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

OT.AC_Pers

238 The security objective **OT.AC_Pers** “Access Control for Personalisation of logical travel document” addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. The write access to the logical travel document data are defined by

the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SOD and, in generally, personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication). If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

OT.Data_Integrity

239 The security objective **OT.Data_Integrity** “Integrity of personal data” requires the TOE to protect the integrity of the logical travel document stored on the travel document’s chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/DH-PACE-AES, FCS_CKM.1/ECDH-PACE-3DES, and FCS_CKM.1/ECDH-PACE-AES and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC).

The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES (for the generation of shared secret andfor the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

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

OT.Data_Authenticity

240 The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself.This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/DH-PACE-AES, FCS_CKM.1/ECDH-PACE-3DES and FCS_CKM.1/ECDH-PACE-AES resp. FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy.The SFR FCS_RND.1 represents a general support for cryptographic operations needed.The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Data_Confidentiality

241 The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp. Chip Authentication, of these data exchanged.This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/DH-PACE-AES, FCS_CKM.1/ECDH-PACE-3DES and FCS_CKM.1/ECDH-PACE-AES resp. FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SOD containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy .The SFR FCS_RND.1 represents the general support for cryptographic operations needed.The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Sense_Data_Conf

242 The security objective **OT.Sense_Data_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

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

OT.Chip_Auth_Proof

243 The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [TR-03110-1] requires additional TSF according to FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES and FCS_CKM.1/CA-ECDH-AES (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

OT.Prot_Abuse-Func

244 The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak

245 The security objective **OT.Prot_Inf_Leak** “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the travel document’s chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or

- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

OT.Tracing

246 The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:(i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) – by FIA_AFL.1/PACE;(ii) for listening to PACE communication (is of importance for the current PP, since SOD is card-individual) – FTP_ITC.1/PACE.

OT.Prot_Phys-Tamper

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

OT.Prot_Malfunction

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

OT.Active_Auth_MRTD_Proof

249 The security objective **OT.Active_Auth_MRTD_Proof** "Proof of MRTD's chip authenticity by Active Authentication" "is covered by the SFRs FCS_COP.1.1/AA_RSA, FCS_COP.1.1/AA_ECDSA, FMT_MTD.1/AA and FMT_MTD.1/KEY_READ.

10.12.3 SFR Dependency Rationale

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

SFR	Dependencies	Support of the Dependencies
FCS_SAS.1	No dependencies	n.a.
FCS_CKM.1/CA-DH-3DES FCS_CKM.1/CA-DH-AES FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation],	Fulfilled by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC,
	FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_CKM.4
FCS_CKM.1/DH-PACE-3DES FCS_CKM.1/DH-PACE-AES FCS_CKM.1/ECDH-PACE-3DES FCS_CKM.1/ECDH-PACE-AES	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]	Fulfilled by FCS_CKM.2/DH

SFR	Dependencies	Support of the Dependencies
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by: FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by: FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES
	FCS_CKM.4 Cryptographic key destruction.	Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by: FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by: FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by: FCS_CKM.1/DH-PACE-3DES FCS_CKM.1/DH-PACE-AES FCS_CKM.1/ECDH-PACE-3DES FCS_CKM.1/ECDH-PACE-AES
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation],	Fulfilled by: FCS_CKM.1/DH-PACE-3DES FCS_CKM.1/DH-PACE-AES FCS_CKM.1/ECDH-PACE-3DES FCS_CKM.1/ECDH-PACE-AES
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/AA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FMT_MTD.1/AA
	FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1/PACE	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1/PACE
FIA_UID.1/PACE	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FDP_RIP.1	No dependencies	n.a.
FDP_UCT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FDP_UIT.1/TRM	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/TRM justification 1 for non-satisfied dependencies
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2 Limited availability	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1 Limited capabilities	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/PA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/AA	FMT_SMF.1 Specification of	Fulfilled by FMT_SMF.1

SFR	Dependencies	Support of the Dependencies
	management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FTP_ITC.1/PACE	No dependencies	n.a.
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TSF.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

Table 9: Dependencies between the SFRs

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

251 No. 1: The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalisation 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.

10.12.4 Security Assurance Requirements Rationale

252 The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the travel document’s development and manufacturing especially for the secure handling of the travel document’s material.

The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

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

The component ALC_DVS.2 has no dependencies.

The component ATE_DPT.2 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_TDS.3 Basic modular design
- ADV_FUN.1 Functional testing

All of these are met or exceeded in the EAL4 assurance package.

The component AVA_VAN.5 has the following dependencies:

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

All of these are met or exceeded in the EAL4 assurance package.

10.12.5 Security Requirements – Mutual Support and Internal Consistency

253 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.

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

255 The dependency analysis in section 10.12.3 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.

256 All subjects and objects addressed by more than one SFR in sec. 10 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items.

257 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 10.12 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.

258 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 10.12.3 Dependency Rationale and 10.12 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 10.12 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.

11. TOE SUMMARY SPECIFICATION

259 The TOE provides the following TOE security functionality, which comply to the [PP-0055]:

- EAC
- PACE
- Active Authentication
- Personalization Agent Authentication
- Secure Messaging
- Access Control
- Cryptographic Support
- Data Protection

260 These Security Functions are implemented by the realisation of the Security Functional requirements, according to chap. 10. The details of the implementation of this TOE security functionality is provided in the following sections.

11.1 SF_EAC – Extended Access Control

261 The TOE implements the Extended Access Control (EAC) mechanism to protects and restricts access to sensitive personal data (EF.DG3, EF.DG4) contained in the TOE chip. In contrast to common personal data (like the bearer's photograph, names, date of birth, etc.) which can be protected by basic mechanisms, more sensitive data (like fingerprints or iris images) must be protected further for preventing unauthorized access and skimming (FDP_UCT.1/TRM, FDP_UIT.1/TRM). The TOE chip protected by EAC will allow that this sensitive data to be read (through an encrypted channel) only by an authorized passport inspection system (FDP_ACF.1/TRM).

The Extended Access Control is a mutual device authentication mechanism defined in [TR-03110-1][ICAO_9303] more precisely, the composition of the Terminal Authentication v.1 protocol and the Chip Authentication v.1 protocol, allows mutual authentication between a terminal and a chip and the establishment of an authenticated and encrypted connection between the TOE and the Inspection System (FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.5/PACE, FIA_API.1, FMT.MTD.3).

The TOE checks by secure messaging in MAC_ENC mode each command whether it was sent by the successfully authenticated terminal (FIA_UAU.6/EAC)

The authentication mechanisms as part of EAC Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging (FDP_ITC.1/PACE).

11.2 SF_PACE – PACE Protocol

262 The TOE implements the PACE protocol with negotiation of session keys (FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/DH-PACE-AES, FCS_CKM.1/ECDH-PACE-3DES, FCS_CKM.1/ECDH-PACE-AES). This protocol provides key component (FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC) to set up a secured channel (FTP_ITC.1/PACE) and to ensure a secure key exchange between the TOE and a terminal. This protocol provides authentication mechanisms implementing the SFRs FIA_UID.1/PACE, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FMT_SMR.1/PACE. The implementation of PACE takes into account the SFR FIA_AFL.1/PACE requirement in order to prevent hacker attacks. The negotiated session keys are used to establish secure channels to protect data confidentiality and integrity during communication implementing the SFR FDP_ITC.1/PACE

11.3 SF_AA – Active Authentication

263 The TOE implements the Active Authentication (AA) mechanism to proof the MRTD chip authenticity according to [ICAO_9303].

264 The Active Authentication cryptographic algorihtm, key length an standards are defined by SFR FCS_COP.1/AA. Algorithm RSA CRT with key length 1024 and 2018 bits. Algorithm ECDSA with key length 192, 224, 256, 320, 384, 512, and 521 bits. For both the algorithms the following hashing algorithms are supported: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

265 The Active Authentication cryptographic key is imported in the TOE by the personalization agent according to the SFR FMT_MTD-1/AA

11.4 SF_AUTH – Personalization Agent Authentication

266 The TOE implements security mechanism to authenticate external entities and assign roles and right.. The purpose of the TSF SF_AUTH is to authenticate the roles of "Personalization Agent" when the TOE is in the life cycle phase 3 "TOE Personalization" (FIA_UAU.4, FIA_UAU.5). The Personalization Agent Authentication Key(s) are pre-loaded in the TOE at the end of phase 2 "TOE Manufacturing". After a succesful authentication the "Personalization Agent" take control of the TOE and execute the steps and operations as described in the life cycle phase 3 "TOE Personalization". The auhentication mechanism is based on challenge-response protocol according to [ICAO_9303] using the AES algorithm and key length of 128, 192 and 256 bits.

11.5 SF_SM - Secure Messaging

267 The TOE implements a trusted channel providing confidentiality and integrity of transferred data according to the FTP.ITC.1/PACE, FIA_UAU.5/PACE, FDP_UCT.1/TRM and FDP_UIT.1/TRM requirements. The trusted channel is using AES and 3DES cipher for encryption in CBC mode and cryptographic key sizes 112, 128, 192 and 256 bits as selected and defined in the SFRs FCS_COP.1/PACE_ENC and FCS_COP.1/CA_ENC. The trusted channel is using a message authentication code generation in CMAC and Retail-MAC mode and cryptographic key sizes 112, 128, 192 and 256 bits as selected and defined in the SFRs FCS_COP.1/PACE_MAC and FCS_COP.1/CA_MAC. The TSF SF_SM uses new fresh random (FCS_RND.1) at each set up of the trusted channel between TOE and terminal.

11.6 SF_AC - Access Control

268 The TOE operates in accordance to the access policies according to FDP_ACC.1/TRM, FDP_ACF.1/TRM and considers the management functions and user roles as defined in FMT_SMF.1 and FMT_SMR.1/PACE respectively.

269 This TSF checks that for each operation initiated by a subject on data (EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD) and keys (Personalization agent key), the security attributes for that roles authorization are satisfied. The function covers the management, write, update and read of stored keys and data as defined in FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/PA and FMT_MTD.1/KEY_READ.

270 The TSF SF_AC access control allows, the user in the role "TOE Manufacturer" during the Phase 2 "TOE Manufacturing" to write the "Initialization Data", which includes but are not limited to the "IC Identification data" and/or "Pre-personalization Data" as required by FAU_SAS.1, to write these data only once.

271 The TSF SF_AC access control allows the users in role Personalisation Agent during the Phase 3 "Personalisation of the travel document" to write in TOE final and genuine personalisation data.

11.7 SF_CRY - Cryptographic Support

272 This TOE Security Function is responsible for providing cryptographic support to all the other TOE Security Functions including secure key generation and operations on data

such as signature generation/verification (FCS_COP.1/SIG_VER), encrypt, decryption, hashing, MAC generation/verification and random number generation:

- The TSF provides all the cryptographic basic mechanisms to implement the EAC protocol Terminal authentication v.1 (FCS_COP.1/SIG_VER):
  - EAC RSA, with 1024 and 2048 bits RSA key, v1.5 and PSS
  - EAC RSA, with SHA-1, SHA-256, and SHA-512
  - EAC ECDSA with 192, 224, 256, 320, 384, 512, and 521 bits EC Key
  - EAC ECDSA with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512

- The TSF provides all the cryptographic basic mechanisms to implement the Chip authentication v.1:
  - DH, with 1024 and 2048 bits DSA key
  - DH, with secure messaging based on DES keys and 128, 192, and 256 bits AES keys
  - ECDH, with 192, 224, 256, 320, 384, 512, and 521 bits EC Key
  - ECDH, with secure messaging based on DES keys and 128, 192, and 256 bits AES keys

- The TSF provides the secure generation of symmetric Key for secure messaging (FCS_CKM.1/DH-PACE-3DES, FCS_CKM.1/ECDH-PACE-3DES, FCS_CKM.1/CA-DH-3DES, FCS_CKM.1/CA-ECDH-3DES). The TSF produces agreed parameters to generate the 3DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [ICAO_9303], Normative appendix A5.1. The algorithm uses the random number generated by TSF as required by FCS_RND.1.
- The TSF provides the secure generation of symmetric Key for secure messaging (FCS_CKM.1/DH-PACE-AES, FCS_CKM.1/ECDH-PACE-AES, FCS_CKM.1/CA-DH-AES, FCS_CKM.1/CA-ECDH-AES). The TSF produces agreed parameters to generate the AES key and the CMAC message authentication keys for secure messaging by the algorithm in [TR-03110-1][ICAO_9303]. The algorithm uses the random number generated by TSF as required by FCS_RND.1.
- The TSF provides high quality Random Number Generator (FCS_RND.1) compliant with the [AIS31/20]. This generator is a deterministic RNG of level DRG.3 according to supporting enhanced backward and forward secrecy.
- The TSF provides Hashing Cryptographic operations SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 for key generation and digital signature generation/verification
- The TSF provides 3DES cipher for encryption/decryption in CBC mode and cryptographic key size 112 bits (FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
- The TSF provides AES cipher for encryption/decryption in CBC mode and cryptographic key size 128, 192 and 256 bits (FCS_COP.1/PACE_ENC, FCS_COP.1/CA_ENC).
- The TSF provides message authentication based on Retail-MAC and cryptographic key size 112 bits (FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
- The TSF provides message authentication based on CMAC and cryptographic key size 128, 192 and 256 bits (FCS_COP.1/PACE_MAC, FCS_COP.1/CA_MAC).
- The TSF provides all the cryptographic basic mechanisms to implement the PACE DH, with Generic Mapping, static or dynamic binding, based on DES keys and 128, 192, and 256 bits AES keys derived from MRZ and CAN.

- The TSF provides all the cryptographic basic mechanisms to implement the PACE ECDH, with Generic Mapping, static or dynamic binding, based on DES keys and 128, 192, and 256 bits AES keys derived from MRZ and CAN.
- The TSF provides support for secure destruction of cryptographic key secret or private material (FCS_CKM.4).

11.8 SF_PRO – Data Protection

273 This TOE Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The TSF SF_RPO Data Protection is composed of software implementations of test and security functions including:

- Performing self-tests of the TOE at each power-up including a set of tests to verify that the underlying cryptographic algorithms are operating correctly (FPT_TST.1)
- Initializing memory after reset
- Initializing memory of de-allocated data and secure destruction of cryptographic key, secrets and private material (FCS_CKM.4, FDP_RIP.1).
- Preserving the TOE lifecycle state integrity to ensure that the testing/debugging features used during development remain irreversibly deactivated for deployment in order to ensure User and TSF Data confidentiality (FMT_LIM.1, FMT_LIM.2).
- Protecting the integrity of all stored cryptographic keys before use and preventing use of corrupted data by stopping the operation involved and setting an error (FCS_CKM.4, FDP_RIP.1).
- Preventing electromagnetic and power emissions or associated information like timing behaviour, in order to preserve the confidentiality of stored keys or residual key material information (FPT_EMS.1).
- Preserving secure state after sensitive processing failure (RNG, power loss, memory or functional failure) or potential physical tampering or intrusion detection (FPT_FLS.1, FPT_PHP.3)

274 This TSF prevents re-activation of de-activated or disabled or terminated mechanisms: the code area and data area are protected (FMT_LIM.1, FMT_LIM.2).

275 This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMS.1).

11.9 Security Functional Requirements coverage

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

SFR vs TSF	SF_EAC – Extended Access Control	SF_PACE - PACE Protocol	SF-AA – Active Authentication	SF_AUTH - Authentication	SF_SM – Secure Messaging	SF_AC – Access Control	SF_CRY – Cryptographic Support	SF_PRO – Data Protection
FAU_SAS.1						x		
FCS_CKM.1/DH-PACE-3DES		x					x	
FCS_CKM.1/DH-PACE-AES		x					x	
FCS_CKM.1/ECDH-PACE-3DES		x					x	
FCS_CKM.1/ECDH-PACE-AES		x					x	

FCS_CKM.1/CA-DH-3DES							x	
FCS_CKM.1/CA-DH-AES							x	
FCS_CKM.1/CA-ECDH-3DES							x	
FCS_CKM.1/CA-ECDH-AES							x	
FCS_CKM.4							x	x
FCS_COP.1/PACE_ENC		x			x		x	
FCS_COP.1/CA_ENC					x		x	
FCS_COP.1/PACE_MAC		x			x		x	
FCS_COP.1/CA_MAC					x		x	
FCS_COP.1/SIG_VER							x	
FCS_COP.1/AA			x					
FCS_RND.1							x	
FIA_AFL.1/PACE		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	x			
FIA_UAU.6/PACE		x						
FIA_UAU.6/EAC	x							
FIA_API.1	x							
FDP_ACC.1/TRM						x		
FDP_ACF.1/TRM	x			x		x		
FDP_RIP.1								x
FDP_UCT.1/TRM	x				x			
FDP_UIT.1/TRM	x				x			
FMT_SMF.1				x		x		
FMT_SMR.1/PACE		x		x		x		
FMT_LIM.1								x
FMT_LIM.2								x
FMT_MTD.1/INI_ENA						x		
FMT_MTD.1/INI_DIS						x		
FMT_MTD.1/CVCA_INI						x		
FMT_MTD.1/CVCA_UPD						x		
FMT_MTD.1/DATE						x		
FMT_MTD.1/CAPK						x		
FMT_MTD.1/AA						x		
FMT_MTD.1/PA						x		
FMT_MTD.1/KEY_READ						x		
FMT_MTD.3	x							
FPT_EMS.1								x
FPT_TST.1								x
FPT_FLS.1								x
FPT_PHP.3								x
FTP_ITC.1/PACE	x	x			x			

Table 10: SFR vs TSF rationale

11.10 Statement of Compatibility

277 This is the statement of compatibility between this Composite Security Target and the Security Target of the underlying javacard platform JSAFE3 [JSAFE3_ST].

11.10.1 Relevance of javacard Platform-ST JSAFE3 TSF

278 Relation of TOE security Function of the Composite-TOE and the javacard Platform-ST JSAFE3:

Javacard Platform JSAFE3 SF Composite TOE SF	SF.CryptoKey	SF.CryptoOp	SF.ObjectDeletion	SF.SecureManagement SF.Transaction SF.SmartCardPlatform apply indirectly to all Composite-TOE security functions
SF_EAC	X	X		X
SF_PACE	X	X		
SF_AA	X	X		X
SF_AUTH	X	X		X
SF_SM		X		X
SF_AC				X
SF_CRY	X	X	X	X
SF_PRO			X	X

279 The SF **SF.PIN** and **SF.Firewall** are considered not relevant to the composite TOE because these functionalities available in javacard platform JSAFE3 are not used by the composite TOE.

11.10.2 Security Requirements

280 The following section verifies that there is no contradiction between the SFRs of the Composite-TOE and the platform JSAFE3. The table below shows the mapping between the javacard platform JSAFE3 SFRs and the Composite ST SFRs. Only the relevant platform JSAFE3 SFRs are listed

Relation of Security Requirements of the Composite-TOE to javacard Platform-ST JSAFE3:

SFR-components of the Composite-TOE	Platform JSAFE3 SFRs
FAU_SAS.1 Audit Storage	-
FCS_CKM.1/DH-PACE-3DES FCS_CKM.1/DH-PACE-AES FCS_CKM.1/ECDH-PACE-3DES FCS_CKM.1/ECDH-PACE-AES FCS_CKM.1/CA-DH-3DES FCS_CKM.1/CA-DH-AES FCS_CKM.1/CA-ECDH-3DES FCS_CKM.1/CA-ECDH-AES Cryptographic key generation	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/SHA - Cryptographic operation fcs_cop.1/DHKeyExchange - Cryptographic operation fcs_cop.1/ECDHKeyExchange - Cryptographic operation fcs_cop.1/DHGMap - Cryptographic operation fcs_cop.1/ECDHGMap - Cryptographic operation
FCS_CKM.4	fcs_ckm.4 Cryptographic key destruction

SFR-components of the Composite-TOE	Platform JSAFE3 SFRs
Cryptographic key destruction - MRTD	
FCS_COP.1/PACE_ENC Cryptographic operation – Encryption / Decryption AES/3DES	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation
FCS_COP.1/PACE_MAC Cryptographic operation – MAC	fcs_cop.1/DES_MAC - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation
FCS_COP.1/CA_ENC Cryptographic operation – Symmetric Encryption / Decryption	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation
FCS_COP.1/CA_MAC Cryptographic operation – MAC	fcs_cop.1/DES_MAC - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation
FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by travel document	fcs_cop.1/RSA_Signature - Cryptographic operation fcs_cop.1/EC Signature - Cryptographic operation
FCS_COP.1/AA Active Authentication	fcs_cop.1/RSA_Signature fcs_cop.1/EC_Signature
FCS_RND.1 Random number generation	fcs_rng.1/DRBG - Generation of random numbers
FIA_AFL.1/PACE Authentication failure handling – PACE authentication using non-blocking authorisation data	-
FIA_UID.1/PACE Timing of identification	-
FIA_UAU.1/PACE Timing of authentication	-
FIA_UAU.4/PACE Single-use authentication mechanism – Single-use authentication of the Terminal by the TOE	fcs_cop.1/DHGMap - Cryptographic operation fcs_cop.1/ECDHGMap - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/RSA_Signature - Cryptographic operation fcs_cop.1/EC Signature - Cryptographic operation
FIA_UAU.5/PACE Multiple authentication mechanisms	fcs_cop.1/DHGMap - Cryptographic operation fcs_cop.1/ECDHGMap - Cryptographic operation fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/DES_MAC - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation fcs_cop.1/RSA_Signature - Cryptographic operation fcs_cop.1/EC Signature - Cryptographic operation
FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE	-
FIA_UAU.6/ EAC Re-authenticating of Terminal by the TOE	-
FIA_API.1 Authentication Proof of Identity	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/DHKeyExchange - Cryptographic operation fcs_cop.1/ECDHKeyExchange - Cryptographic operation
FDP_ACC.1 Subset access control – Basic Access Control	-
FDP_RIP.1 Subset residual information protection	fdp_rip.1/ABORT - Subset residual information protection fdp_rip.1/bArray - Subset residual information protection fdp_rip.1/KEYS - Subset residual information protection fdp_rip.1/TRANSIENT - Subset residual information protection
FDP_UCT.1/TRM Basic data exchange confidentiality - MRTD	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation
FDP_UIT.1/TRM Data exchange integrity - MRTD	fcs_cop.1/DES_MAC - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation
FDP_ACC.1/TRM	-

SFR-components of the Composite-TOE	Platform JSAFE3 SFRs
Subset access control	
FDP_ACF.1/TRM Security attribute based access control control - Basic Access Control	-
FMT_SMF.1 Specification of management functions	-
FMT_SMR.1/PACE Security roles	-
FMT_LIM.1 Limited capabilities	fmt_lim.1/Test - Limited capabilities
FMT_LIM.2 Limited availability	fmt_lim.2/Test - Limited availability
FMT_MTD.1/INI_ENA Management of TSF data – Writing of initialization data and personalization data	-
FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data	-
FMT_MTD.1/PA Management of TSF data – Personalization Agent	-
FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date	-
FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifying Certification Authority	-
FMT_MTD.1/DATE Management of TSF data – Current date	-
FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key	-
FMT_MTD.1/AA Management of TSF data – Active Authentication Private Key	-
FMT_MTD.1/KEY_READ Management of TSF data – Key Read	-
FMT_MTD.3 Secure TSF data	-
FTP_ITC.1/PACE Inter-TSF trusted channel after PACE	fcs_cop.1/DES-TDES_Cipher - Cryptographic operation fcs_cop.1/AES_Cipher - Cryptographic operation fcs_cop.1/DES_MAC - Cryptographic operation fcs_cop.1/AES_CMAC - Cryptographic operation
FPT_EMS.1 TOE emanation	fpt_emsec.1 TOE Emanation
FPT_FLS.1 Failure with preservation of secure state	fpt_fls.1/Operate - Failure with preservation of secure state
FPT_TST.1 TSF testing	fpt_tst.1 - TSF testing
FPT_PHP.3 Resistance to physical attack	fpt_php.3 - Resistance to physical attack

Platform-SFRs classification

IP_SFR : Irrelevant Platform-SFRs:

fcs_ckm.1/RSA	fcs_ckm.1/EC	fcs_ckm.1/DSA	fcs_ckm.2/DES
fcs_ckm.2/AES	fcs_ckm.2/RSA_STD	fcs_ckm.2/RSA_CRT	fcs_ckm.2/EC
fcs_ckm.2/DSA	fcs_ckm.3/DES	fcs_ckm.3/AES	fcs_ckm.3/RSA_STD
fcs_ckm.3/RSA_CRT	fcs_ckm.3/EC	fcs_ckm.3/DSA	fcs_cop.1/RSA_Cipher
fcs_cop.1/ECDH_KeyExchange	fcs_cop.1/DH_KeyExchange	fcs_rng.1/IC	

RP_SFR-SERV: Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.

fcs_ckm.4	fcs_cop.1/DES-TDES_Cipher	fcs_cop.1/DES_MAC	fcs_cop.1/AES_Cipher
fcs_cop.1/AES_MAC	fcs_cop.1/AES_CMAC	fcs_cop.1/RSA_Signature	fcs_cop.1/EC_Signature
fcs_cop.1/SHA	fcs_cop.1/ECDHGMap	fcs_cop.1/DHGMap	fcs_rng.1/DRBG
fpt_fls.1/Operate	fpt_php.3	fpt_tst.1	fpt_emsec.1

RP_SFR-MECH: Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

fdp_acc.2/FIREWALL	fdp_acf.1/FIREWALL	fdp_ifc.1/JCVM	fdp_iff.1/JCVM
fdp_rip.1/OBJECTS	fmt_msa.1/JCRE	fmt_msa.1/JCVM	fmt_msa.2/FIREWALL_JCVM
fmt_msa.3/FIREWALL	fmt_msa.3/JCVM	fmt_smf.1	fmt_smr.1
fdp_rip.1/ABORT	fdp_rip.1/APDU	fdp_rip.1/bArray	fdp_rip.1/KEYS
fdp_rip.1/TRANSIENT	fdp_rol.1/FIREWALL	fau_arp.1/JCS	fdp_sdi.2
fpr_uno.1/PIN	fpr_uno.1/KEY	fpt_fls.1	fpt_tdc.1
fia_atd.1/AID	fia_uid.2/AID	fia_usb.1/AID	fmt_mtd.1/JCRE
fmt_mtd.3/JCRE	fdp_rip.1/ODEL	fpt_fls.1/ODEL	fdp_acc.1/GP_API
fdp_acf.1/GP_API	fmt_msa.1/GP_API	fmt_msa.3/GP_API	fmt_smr.1/GP_API
fia_uid.1/GP_API	fdp_acc.1/Atomicity	fdp_rol.1/Atomicity	fru_flt.2
fpt_fls.1/SCP	fmt_lim.1/Test	fmt_lim.2/Test	fdp_sdc.1
fdp_sdi.2	fdp_itt.1	fpt_itt.1	fdp_ifc.1

Security Assurance Requirements

281 The chosen level of assurance of the javacard platform-ST JSAFE3 is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5.

282 The Assurance Requirement levels of Composite-TOE is EAL4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. There is no contradiction between the Assurance Requirements for the Composite-TOE and the underlying platform-ST JSAFE3.

11.10.3 Security Objectives

283 The following section verifies that there is no contradiction between the Security Objectives of the Composite-TOE and the javacard platform-ST JSAFE3.

<u>Relation of the Security Objectives of the Composite-ST and the javacard platform-ST JSAFE3:</u>

Javacard platform-ST JSAFE3 Security Objectives Composite-ST Security Objectives	*O.OPERATE*	*O.REALLOCATION*	*O.SCP.RECOVERY*	*O.SCP.IC*	*O.SCP.SUPPORT*	*O.CIPHER*	*O.KEY-MNGT*	*O.TRANSACTION*	*O.OBJ-DELETION*	*O.SIDE_CHANNEL*	*O.GLOBAL_ARRAY_CONFID*
OT.Sens_Data_Conf				x		x	x		x	x	
OT.Chip_Auth_Proof				x							
OT.AC_Pers					x	x					
OT.Data_Integrity			x			x	x	x			
OT.Data_Authenticity						x	x				
OT.Data_Confidentiality						x	x				
OT.Tracing										x	
OT.Prot_Abuse-Func		x					x	x	x		x
OT.Prot_Inf_Leak				x						x	
OT.Identification					x						
OT.Prot_Phys-Tamper				x						x	
OT.Prot_Malfunction	x		x	x						x	
OT.Active_Auth_MRTD_Proof						x	x				

284 Security Objectives for the javacard platform JSAFE3 not relevant for the Composite-TOE:

O.ALARM, O.SID, O.ROLES, O.GLOBAL_ARRAYS_INTEG, O.GLOBAL_ARRAYS_CONFID, O.NATIVE, O.LIFE_CYCLE, O.RESOURCES , O.FIREWALL, O.PIN-MNGT

11.10.4 Security Objectives for the Environment

285 The following section verifies that there is no contradiction between the Security Objectives for the envornment for the Composite-TOE and for the javacard platform-ST JSAFE3.

IrOE: The objectives for the environment being not relevant for the Composite-ST are the following: none

CfPOE: The objectives for the environment being fulfilled by the Composite-ST automatically are the following: none

SgOE: The objectives for the environment significant for the Composite-ST are the following:

- OE.CARD_MANAGEMENT, OE.NO-DELETION, OE.NO-INSTALL, OE.VERIFICATION, OE.CODE-EVIDENCE. All these objectives are relevant to the composite TOE because a correct verification and management of the TOE applet code (JSAFE3_EPASS V.3.0.4 and IAS V.2.0.3) before and after installation is crucial and necessary for the TOE security.

Note: The status of the platform Card Manager (also called Issuer Security Domain, ISD) is locked in post-issuance i.e. applet loading, installation and deletion is no more possible.

- OE.MANAGEMENT_OF_SECRETS. User secret or TSF data managed outside the TOE shall be protected against unauthorised disclosure and modification. This objective is enforced by **OE.Personalization** stated for the composite TOE.

11.10.5 Compatibility: TOE Security Environment

11.10.5.1. Assumptions

286 The following section verifies that there is no contradiction between the Assumptions of the Composite-ST and the javacard platform-ST JSAFE3

Assumptions for the Composite-TOE referring to the MRTD operational capabilities only:

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

Assumptions of the javacard platform-ST JSAFE3 are not referring to Composite-TOE assumptions:

- A.VERIFICATION: All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.
- A.NO-DELETION: No deletion of installed applets (or packages) is possible.
- A.NO-INSTALL: There is no post-issuance installation of applets. Installation of applets is secure and occurs only in a controlled environment in the pre-issuance phase.

11.10.5.2. Threats

287 The following section verifies that there is no contradiction between the Threats of the Composite-TOE and the javacard platform-ST JSAFE3.

Threats for the Composite-TOE:

- **T.Read_Sensitive_Data** - Read the sensitive biometric reference data
- **T.Counterfeit** - Counterfeit of travel document chip data
- **T.Skimming** - Skimming travel document / Capturing Card-Terminal Communication
- **T.Eavesdropping** - Eavesdropping to the communication between TOE and inspection system
- **T.Tracing** - Tracing travel document
- **T.Abuse-Func** - Abuse of Functionality
- **T.Information_Leakage** - Information Leakage from MRTD's chip
- **T.Phys-Tamper** - Physical Tampering
- **T.Malfunction** - Malfunction due to Environmental Stress
- **T.Forgery** - Forgery of data on MRTD's chip

Threats of the javacard platform-ST JSAFE3:

- T.OBJ-DELETION: The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application.
- T.INTEG-APPLI-DATA: The attacker executes an application to alter (part of) another application's data.

- T.CONFID-APPLI-DATA: The attacker executes an application to disclose data belonging to another application.
- T.CONFID-JCS-DATA: The attacker executes an application to disclose data belonging to the Java Card System.
- T.INTEG-JCS-DATA: The attacker executes an application to alter (part of) Java Card System or API data or the SCP data.
- T.SID.1: A fake applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the TOE or with respect to the end user or the terminal.
- T.SID.2: The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role.
- T.RESOURCES: An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.
- T.PHYSICAL: The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques. This threatens all the identified assets.

  Refinement:
  This threat also addresses leakage of information that may occur during TOE usage through:
    - Emanations,
    - Variations in power consumption,
    - I/O characteristics,
    - Clock frequency,
    - Changes in processing time

- T.LIFE_CYCLE: An attacker accesses to product functionalities outside of their expected availability range thus violating irreversible life cycle phases of the product (for instance, an attacker downloads, install, or delete applications available on the product at post-issuance).

288 There are no contradictions between the threats of the composite TOE and the threats of the underlying javacard platform-ST JSAFE3.

11.10.5.3. Organizational Security Policies

289 The following section verifies that there is no contradiction between the OSPs of the Composite-TOE and the javacard platform-ST JSAFE3.

Organizational Security Policies of the Composite-TOE:

- **P.Sensitive_Data** - Privacy of sensitive biometric reference data
- **P.Personalisation** - Personalisation of the travel document by issuing State or Organisation only
- **P.Pre-Operational** - Pre-operational handling of the travel document
- **P.Card_PKI** - PKI for Passive Authentication (issuing branch)
- **P.Trustworthy_PKI** - Trustworthiness of PKI
- **P.Manufact** - Manufacturing of the MRTD's chip
- **P.Terminal** - Abilities and trustworthiness of terminals
- **P.Active_Auth –** Active Authentication

Organizational Security Policies of the javacard platform-ST JSAFE3:

- OSP.VERIFICATION: This policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority.
- OSP.MANAGEMENT_OF_SECRETS: Management of secret data (e.g. generation, storage, distribution, destruction, loading into the product of cryptographic private keys, symmetric keys and user authentication data) performed outside the product on behalf of the TOE or Product Manufacturer shall comply with security organisational policies that enforce integrity and confidentiality of these data. Secret data shared with the user of the product shall be exchanged through trusted channels that protect the data against unauthorised disclosure and modification and allow detecting potential security violations.

- OSP.ROLES: The TOE shall recognize the following roles associated with:
    - Applications

- OSP.CARD_ADMINISTRATION_DISABLED: Card Content Management Functions (CCMFs) shall not be available after TOE delivery.

290 No organizational security policies of underlying javacard platform-ST JSAFE3 is mapped to platform relevant objectives.

291 There are no contradictions between the organizational security policies of the composite TOE and the organizational security policies of the underlying javacard platform-ST JSAFE3.

11.10.6 Conclusion

292 There are no contradictions between the ST of the composite TOE and the ST of the underlying javacard platform-ST JSAFE3.

12. ANNEX A – CRYPTO DISCLAIMER

293 The following cryptographic algorithms are used by the TOE to enforce its security policy:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits
Authentication	AES in CBC mode	[FIPS_PUB_197] (AES), [ISO 10116] (CBC) [ICAO_9303] chap. 4.3	Key sizes: 128, 192 and 256 bits
	RSA in CRT	[ISO_9796-2]	1024, 2048 bits
	ECDSA	[TR-03111]	192,224,256,320,384,512 and 521
Key Agreement	Session key established with EAC Terminal Authentication protocol v.1 Session key established with EAC Chip Authentication protocol v.1 Session key established with PACE protocol	[ICAO_9303] [TR-03110-1]	Key sizes: 112,128,192 and 256 bits
Confidentiality	3DES in CBC mode	[FIPS_46_3] and [ICAO_9303] normative appendix 5, A5.3	Key sizes: 112 bits
	AES in CBC mode	[FIPS_PUB_197] (AES), [ISO 10116] (CBC)	Key sizes: 128,192 and 256 bits
Integrity	Symmetric: Retail-MAC CMAC	[ISO-9797-1] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [SP800-38B] [RFC4493]	Symmetric Key sizes: 112 for retail-MAC Symmetric Key sizes: 128,192 and 256 bits for CMAC
	Asymmetric: RSA ECDSA	[PKCS1_v1_5] [RFC3447] [ANSI_X9.62] [TR-03111]	Asymmetric key sizes: 1024, 2048 bites for RSA keys. Asymmetric key sizes: 192, 224, 256, 320, 384, 512, and 521 bits for ECDSA keys
Trusted Channel	Secure messaging in ENC_MAC mode and key established with EAC protocol	[ICAO_9303]	Key sizes: 112,128,192 and 256 bits
RNG	True Random Generator (TRNG) class PTG.2 Deterministic Random Generator (DRBG) class RNG DRG.3	[AIS31/20]	N.A.
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS_180-2]	N.A.

13. QUALITY REQUIREMENTS

13.1 Revision History

Version	**Subject**
A	Initial Release – 13-March-2019

Table 11 - Revision History

14. ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.