eTravel v2.3 on MultiApp v4.1 platform PACE, EAC and AA activated

Security Target Lite

Date	Author	
July 5th 2018	Gemalto	Created from evaluated ST (V1.5)

CONTENT

FIGURES

TABLES

1. SECURITYTARGET INTRODUCTION

1.1 SECURITY TARGET REFERENCE

Title :	MultiApp V4.1 eTravel 2.3 EAC on SAC Security Target
Version :	1.5p
ST Reference :	D1417547
Author :	Gemalto
IT Security Evaluation scheme :	Serma Safety and Security
IT Security Certification scheme:	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 TOE REFERENCE

Product Name :	eTravel 2.3 (MultiApp V4.1)
Security Controllers :	S3FT9MH
TOE Name :	eTravel 2.3 EAC/SAC on MultiApp V4.1
TOE Reference :	eTravel 2.3 EAC/SAC Release 1.0
TOE documentation :	Guidance [AGD]
Composition elements:	
IC TOE identifier:	S3FT9MH/S3FT9MV/S3FT9MG
IC TOE Version:	S3FT9MH/S3FT9MV/S3FT9MG_rev0-1_SW10-49-50-70-10-103-202_GU113-16-005-201-133-24-22-24-14

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD). These data are available by executing a dedicated command.

The TOE and the product differ, as further explained in §2 TOE :

- The TOE is the eTravel 2.3 application on MultiApp V4.1.
- The MultiApp V4.1 product also includes other applets.

1.3 SECURITY TARGET OVERVIEW

This Security Target defines the security objectives and requirements for the contact/contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control and Extended Access Control as well as the advanced authentication mechanisms Chip Authentication and Active Authentication.

The Security Target is based on Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control* [PP-MRTD-EACV2].

The Security Target defines the security requirements for the TOE. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the MRTD application and data during its life cycle.

The main objectives of this ST are:

- To introduce TOE and the MRTD application,
- To define the scope of the TOE and its security features,
- To describe the security environment of the TOE, including the assets to be protected and the threats to be countered by the TOE and its environment during the product development, production and usage.
- To describe the security objectives of the TOE and its environment supporting in terms of integrity and confidentiality of application data and programs and of protection of the TOE.
- To specify the security requirements which includes the TOE security functional requirements, the TOE assurance requirements and TOE security functions.

1.4 REFERENCES

1.4.1 External References

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation Evaluation Methodology CCMB-2017-04-004, version 3.1 rev 5, April 2017
[RGS-B1]	Référentiel Général de sécurité version 2 Annexe B1 Mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques; version 2.0.3 du 21 février 2014
[AIS20/31]	A proposal for : Functionality classes for random number generators Version 2.0, 18/09/2011
[SP 800-90]	NIST Special Publication 800-90A, Revision 1, Recommendation for the Random Number Generation Using Deterministic Random Bit Generators, June 2015
[SMG-IC]	[SMG-IC-9MH]
[SMG-IC-9MH]	ST of S3FT9MH – version 3.2 , 27th March 2017
[CR-IC-9MH]	[CR-IC-9MH]
[CR-IC-9MH]	*Certification Report*, S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software ANSSI-CC-2017/24, 11/05/2017
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO9796-2]	*ISO/IEC 9796-2:2010: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms,* Third edition 2010-12-15
[ISO9797-1]	*ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* Second edition 2011-03-01
[ICAO-9303]	9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 1-12
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	9303 ICAO Machine Readable Travel Document 7th edition, 2015 Part 11-12
[PP-IC-0084]	Security IC Platform Protection Profile with augmentation Packages– BSI-CC-PP-0084-2014
[PP-MRTD-EACV2]	Protection Profile, Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, version 1.3.2, 2012, December 5th. Certified and maintained by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0056-V2-MA-2012.

[PP-MRTD-SAC]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.01, 22 juillet 2014. Certified and maintained by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-CC-PP-0068-V2-2011-MA-01.
[PP-MRTD-BAC]	Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 mars 2009. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0055-2009.
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010-03M01, Version 3.0, May 2012
[SS]	*ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS*, *Excerpts from ICAO Doc 9303, Part 1* Machine Readable Passports, Fifth Edition – 2003
[TR-ECC]	Elliptic Curve Cryptography according to ISO 15946, Technical Guideline, TR-ECC, BSI, 2006
[TR-EAC-1]	Technical Guideline – TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015
[BIO]	BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004

1.4.2 Internal References

[ST-EAC SAC]	D1417547 eTravel 2.3 EAC on SAC Security Target - MultiApp V4.1
[ST-BAC]	D1417545 BAC Security Target - MultiApp V4.1
[ST-Platform]	D1417544, MultiApp V41: JCS Security Target
[AGD]	Guidance Documentation
[AGD-Ref]	eTravel v2.2 and 2.3 Reference Manual Ref. D1392378, August 24,2017
[AGD-GDP]	Global Dispatcher Personalization Applet User guide Ref. D1390286H, April 6, 2018
[AGD-OPE]	MultiApp V4.1: AGD OPE document - eTravel v2.3 Ref. D1425961, Ver 1.1, June 20th, 2018
[AGD-PRE]	MultiApp V4.1: AGD PRE document - eTravel v2.3 Ref. D1425962, Ver 1.0, 05/06/2017
[Applet guidance]	Guidance for secure application development on Multiapp platforms, D1390326 Rev. A01, March 2018
	Verification process of Gemalto non sensitive applet, D1390670 Rev. A01, Feb 2016
	Verification process of Third Party non sensitive applet, D1390671 Rev. A01, Feb 2016
	Rules for applications on Multiapp certified product, D1390963 Rev. 1.2, Nov 2017

2. TOE OVERVIEW

2.1 TOE DESCRIPTION

The TOE is the module designed to be the core of an MRTD passport. The TOE is a contact/contactless integrated circuit. The TOE is connected to an antenna and capacitors and is mounted on a plastic film. This inlay is then embedded in the coversheet or datapage of the MRTD passport and provides a contactless interface for the passport holder identification.

The Target of Evaluation (TOE) is the contact/contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [ICAO-9303] and providing:

- the Basic Access Control (BAC) according to the ICAO document [PKI]
- the Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]
- the PACE V2 Access Control (SAC) according to the ICAO document [ICAO-TR-SAC]
- the Extended Access Control according to the BSI document [TR-EAC-1]

Additionally to the [PP-MRTD-EACV2], the TOE has a set of administrative commands for the management of the product during the product life.

The TOE comprises of at least

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the eTravel v2.3 application on MultiApp v4.1 Open Platform.
- The GDP Applet
- The associated guidance documentation.
- A cryptographic library developed by Gemalto (the cryptographic library proposed by the chip supplier is not used).

The MultiApp v4.1 is an open platform [ST-Platform].

The TOE delivery:

The TOE can be delivered under 2 configurations:

- ✓ The configuration called "Standalone" meaning the eTravel 2.3 is the only applet selectable on the platform (GP221 "Final application" privilege).
- ✓ The configuration called "Open" meaning eTravel 2.3 is selectable among other applets on the platform.

The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition, the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent. The Personalization Key is generated on the Manufacturing Site and transmitted to the Personalization Agent through a secured method (Key Ceremony involving Security Agents on a dedicated secure environment with KMS devices). Depending on customer needs and preferences, the Personalization Key could also be generated on the Personalization Agent side (dedicated secure environment with KMS devices) and transmitted to the Manufacturing site through a secure method (Key Ceremony involving Security Agents) in order to be integrated to the TOE.

2.2 TOE BOUNDARIES

The eTravel 2.3 EAC/SAC on MultiApp V4.1 Embedded Software (ES) is located in the flash code area.

The figure below gives a description of the TOE and its boundaries (red dash line)

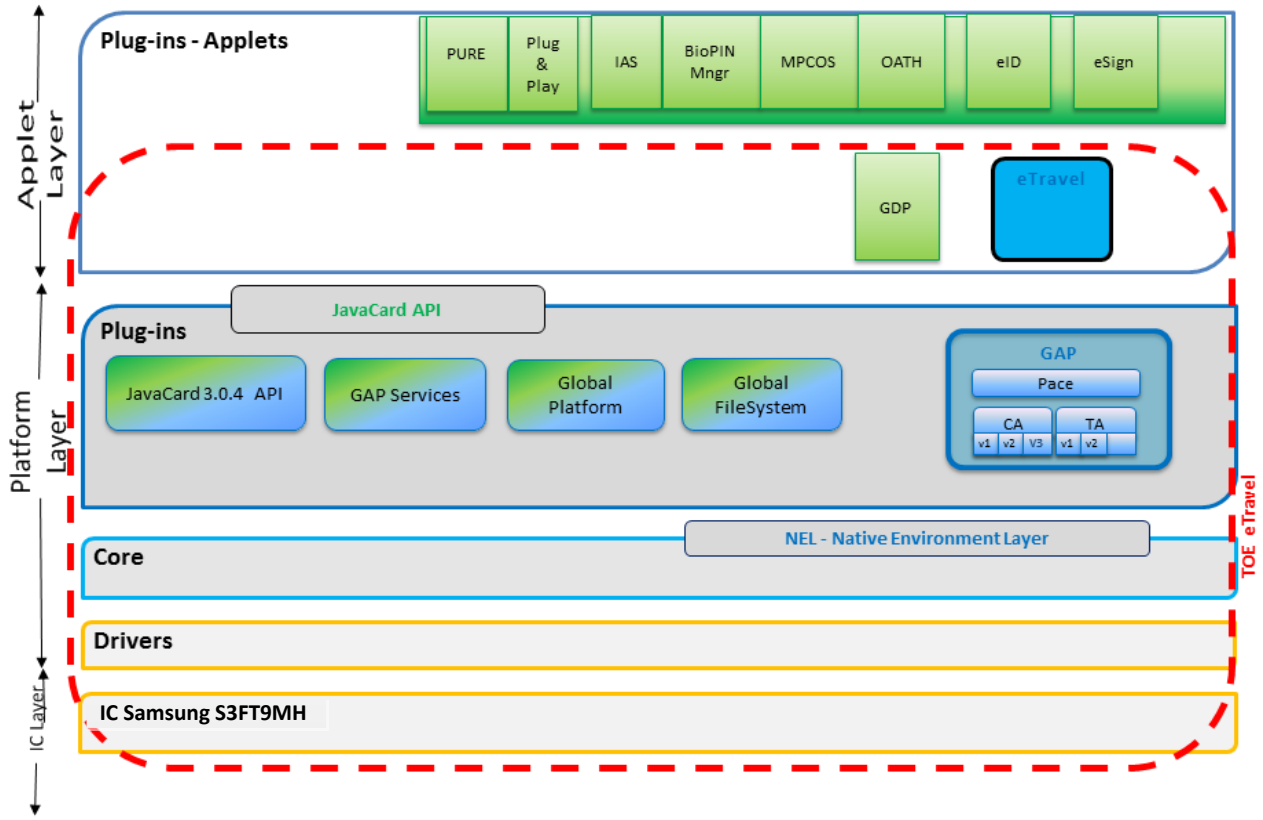


Figure 1: TOE Boundaries

2.3 TOE USAGE AND SECURITY FEATURES FOR OPERATIONAL USE

A State or Organization issues MRTDs to be used by the holder for international travel. The traveller presents an MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip 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.
The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. Receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

(a) the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
  (1) the biographical data on the biographical data page of the passport book,
  (2) the printed data in the Machine Readable Zone (MRZ) and
  (3) the printed portrait.

(b) the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
  (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  (2) the digitized portraits (EF.DG2),
  (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both,
  (4) the other data according to LDS (EF.DG5 to EF.DG16) and
  (5) the Document security object.

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 is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303]. These security measures include the binding of the MRTD's chip to the passport book.

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 MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [ICAO-9303] and Password Authenticated Connection Establishment [TR-SAC]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This security target addresses the Chip Authentication Version 1 described in [TR-EAC-1] as an alternative to the Active Authentication stated in [ICAO-9303].

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

The confidentiality Password Authenticated Connection Establishment (PACE) is a mandatory security feature that shall be implemented by the TOE, too. The MRTD has additionally to fulfil the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-BAC-MRTD].

For PACE protocol according to [TR-SAC] , the following steps shall be performed :
(i) the MRTD encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.

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

(iii) The MRTD and the terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the shared secret.
(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the MRTD provide private communication (secure messaging) [TR-SAC], [TR-EAC-1].

The security target requires the TOE to implement the Chip Authentication defined in [TR-EAC-1]. The Chip Authentication prevents data traces described in [ICAO-9303], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [TR-EAC-1]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization 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 Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

The security target also requires the TOE to implement Active Authentication as defined in [ICAO-9303].

Keys for Chip authentication and Active Authentication can be generated in the card or loaded into it. These operations take place at personalization time.

2.4 TOE LIFE-CYCLE

2.4.1 Actors

Actors	Identification
Integrated Circuit (IC) Developer	Samsung
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	Samsung
Module manufacturer	Gemalto
Pre-personalizer	Gemalto
Inlay manufacturer	Gemalto or another Inlay manufacturer
Book manufacturer	Gemalto or another printer
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalize the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 1: Identification of the actors

2.4.2 TOE Life Cycle

Phase (name)	Step	Actor	Comment
Development	1. MRTD application Development	Developer (Gemalto)	- The development of the MRTD application is integrated in the platform MultiApp V4.1. -Generation of flash image, mapping description - Script generation for initialization and pre-personalization
	2 HW Development	IC manufacturer (Samsung)	- Development of IC
Manufacturing	3 Mask manufacturing	IC manufacturer (Samsung)	Manufacturing of virgin chip integrated circuits embedding the Samsung flash Loader and protected by a dedicated transport key.
	4 Module manufacturing	Module creation (Gemalto or Samsung)	IC packaging & testing
	5.a Embedding	*Form factor manufacturer (optional)(Gemalto or other)*	*Put the module on a dedicated form factor (Card, Inlay, other)*
	5.b Initialization / Pre-personalization	manufacturer (Gemalto)	Loading of the Gemalto software (platform and applets on top of it based on script generated)
	5.c Embedding if not done during 5.a	*Form factor manufacturer (optional)(Gemalto or other)*	*Insert/embed the module into a dedicated form factor (Card, Inlay, other)*
Personalization	6 Personalization	Personalizer	- Personalization
Usage	7 Usage	Holder	- The Issuer is responsible of card delivery to the end-user

Remarks:

1. Initialization & pre-personalization operation could be done on module or on other form factor. The form factor does not affect the TOE security.
2. Alternative life cycle: wafers are shipped by Samsung to form factor manufacturer (no module manufacturing required) and initialization /pre-personalization is done in Gemalto site.
3. For initialization/pre-personalization IC flash loader could be used based on the IC manufacturer recommendation.
4. Embedding (module inserted in the final form factor) will be done on an audited site.
5. TOE delivery is done after Step 5 – The Red Dash Line represents the TOE development

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

Phase 1 “Development”:

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.
As a result a flash mask is generated (HEX file) with initialisation and pre-personalisation scripts.

Phase 2 “Manufacturing”:

(Step3) In a first step the IC manufacturer produce virgin chip with IC Identification Data and the flash loader software. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.
(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book
(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.
The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 “Personalization of the MRTD”:

(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder’s biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.

The signing of the Document security object by the Document signer [5] 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.

Phase 4 “Operational Use”

(Step7) The TOE is used as MRTD chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

As a summary description of how the parts of the TOE are delivered to the final customer, the eTravel v2.3 on MultiApp v4.1 application is delivered mainly in form of a smart card or inlay. The form factor is packaged on Gemalto’s manufacturing facility and sent to final customer premises.

The different guides accompanying the TOE and parts of the TOE are the ones specified in [AGD] section. They are delivered in form of electronic documents (*.pdf) by Gemalto’s Technical representative.

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

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna, the booklet or card (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

3. CONFORMANCE CLAIMS

3.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to been taken into account.

3.2 PP CLAIM,

The MultiApp V4.1 eTravel 2.3 EAC/SAC security target claims strict conformance to the Protection Profile [PP-MRTD-EACV2].
[PP-MRTD-EACV2] claims strict conformance to [PP-MRTD-SAC].

The MultiApp V4.1 eTravel 2.3 EAC/SAC security target is a composite security target, including the IC security target [SMG-IC]. However the security problem definition, the objectives, and the SFR of the IC are not described in this document.

3.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC-3].

3.4 CONFORMANCE STATEMENT

This ST strictly conforms to [PP-MRTD-EACV2].

4. SECURITY PROBLEM DEFINITION

4.1 INTRODUCTION

Assets
The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in §9 Glossary and acronyms for the term definitions)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
travel document			
1	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-SAC] 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-SAC]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [PP-MRTD-BAC].	Confidentiality[1] Integrity Authenticity
2	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-SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). User data can be received and sent (exchange Û {receive, send}).	Confidentiality[2] Integrity Authenticity
3	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 PAC E password. TOE tracing data can be provided / gathered.	unavailability[3]

Table 2: Primary assets

*Application note***:** Sensitive biometric reference data (EF.DG3, EF.DG4) are included in Object 1.

All these primary assets represent User Data in the sense of the CC.

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

[1] Though not each data element stored on the TOE represents a secret, the specification [ICAO-TR-SAC] anyway requires securing their confidentiality: only terminals authenticated according to [ICAO-TR-SAC] can get access to the user data stored. They have to be operated according to P.Terminal.
[2] Though not each data element being transferred represents a secret, the specification [ICAO-TR-SAC] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [ICAO-TR-SAC].
[3] represents a prerequisite for anonymity of the travel document holder

Object No.	Asset	Definition	Property to be maintained by the current security policy
travel document			
4	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.	Availability
5	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-MRTD-BAC].	Availability
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	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.	Integrity Authenticity
8	travel document communication establishment authorisation data	Restricted-revealable[4] 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.	Confidentiality Integrity

Table 3: Secondary assets

The secondary assets represent TSF and TSF-data in the sense of the CC.

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

A sensitive asset is the following more general one.

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.

Subjects

This security target considers the following external entities and subjects, defined in [PP-MRTD-SAC]]:

[4] The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorized person or device who definitely act according to respective regulations and are trustworthy.

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalised the travel document[5]. This entity is commensurate with 'MRTD Holder' in [ST-BAC]. Please note that a travel document holder can also be an attacker (s. below).
2	-	travel document presenter (traveller)	A person presenting the travel document to a terminal[6] and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [ST-BAC]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	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 [ST-BAC].
-	-	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.
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[7] 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. See also §2.4.3 above.
-	-	Extended Inspection System (EIS)	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 Version 1 according to [TR-EAC-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.
5	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document

[5] i.e. this person is uniquely associated with a concrete electronic Passport
[6] in the sense of [4]
[7] concretely, by a control officer

External Entity No.	Subject No.	Role	Definition
			for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [PKI]. This role is usually delegated to a Personalisation Agent.
6	-	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 (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [PKI], 5.5.1.
7	4	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 [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (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. This entity is commensurate with 'Personalisation agent' in [ST-BAC].
8	5	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 phase[8]. 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 [ST-BAC].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying (i) to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained, (ii) to manipulate the logical travel document without authorization, (iii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iv) to forge a genuine travel document, or (iv) to trace a travel document. 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 [ST-BAC].
10	-	Country Verifying Certification Authority (CVCA)	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

[8] cf. also par. 1.2.3 in sec. 1.2.3 above

External Entity No.	Subject No.	Role	Definition
			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.
11	-	Document Verifier (DV)	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.

Table 4: Subjects and external entities[9]

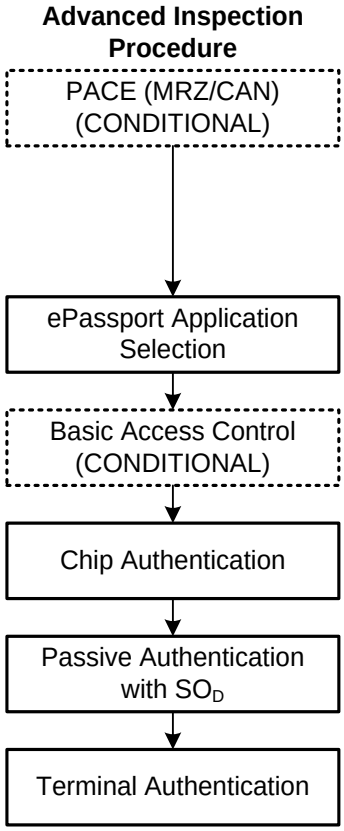


Figure 2: Advanced Inspection Procedure

[9] This table defines external entities and subjects in the sense of [CC-1] . Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC-1]). From this point of view, the TOE itself perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any
subject role recognised by the TOE.

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

4.2 ASSUMPTIONS

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

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 [PKI].

A.Insp_Sys Inspection Systems for global interoperability
The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO-TR-SAC] and/or BAC [ST-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 [[PP-MRTD-SAC] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the EAC functionality of the TOE.

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 [PP-MRTD-SAC] 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 Version 1.

4.3 THREATS

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

The TOE in collaboration with its IT environment shall avert the threats as specified below.

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: When using BIS-BAC MultiApp V4.1 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.

T.Eavesdropping Eavesdropping on the communication between the TOE and the PACE terminal

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 travel document data

Application Note: When using BIS-BAC MultiApp V4.1 cannot avert this threat in the context of the security policy defined in this PP.

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 [ST--BAC].

Application Note: When using BIS-BAC MultiApp V4.1 cannot avert this threat in the context of the security policy defined in this PP, see also §2.4.3 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)[10] cannot be averted by the current TOE.

T.Forgery Forgery of Data

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 (or EAC) authenticated BIS-PACE (or EIS) 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

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.

T.Information_Leakage Information Leakage from travel document

[10] Such a threat might be formulated like: ‘An attacker produces an unauthorised copy or reproduction of a *genuine* travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of a travel document presenter as the travel document holder’.

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).

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:	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.

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.

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 (cf. [ST-BAC]) 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)

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

This ST includes all threats from the [PP-MRTD-SAC], chap 3.2, namely T.Skimming, T.Eavesdropping, T.Tracing, T.Abuse-Func, T.Information_Leakage, T.Phys-Tamper, T.Forgery and T.Malfunction. Due to identical definitions and names they are not repeated here as well.

Application note:
T.Forgery from the [PP-MRTD-SAC] shall be extended by the Extended Inspection System additionally to the PACE authenticated BIS-PACE being outsmarted by the attacker.

4.4 ORGANIZATIONAL SECURITY POLICIES

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

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.

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

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

2.) 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[11].

3.) 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, cf. sec. 1.2.3 above.

4.) 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.

P.Card_PKI PKI for Passive Authentication (issuing branch)

Application Note 20: 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 (C_{CSCA}).

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 (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [PKI] , 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [PKI], 5.5.1.

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.

P.Trustworthy_PKI Trustworthiness of PKI

[11] cf. Table 2 and Table 3 above

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

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, cf. above) shall be used by terminal operators and by travel document holders as defined in [PKI].

2.) They shall implement the terminal parts of the PACE protocol [ICAO-TR-SAC], of the Passive Authentication [PKI] and use them in this order[12]. 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 C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [PKI]).

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 according to the current PP.

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 Version 1.

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.

P.Active_Auth Active Authentication

The TOE implements the active authentication protocol as described in [ICAO-9303].

[12] This order is commensurate with [ICAO-TR-SAC].

4.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-EAC SAC] AND [SMG-IC]

4.5.1 Compatibility between threats of [ST-EAC SAC] and [SMG-IC]

T.Read_Sensitive_Data, is included in T.Phys-Probing.
T.Forgery is included in T.Phys-Manipulation.
T.Abuse-Func of [ST-EAC SAC] is included in T.Abuse-Func of [SMG-IC].
T.Information_Leakage is included in T.Leak-Inherent and T.Leak-Forced.
T.Phys-Tamper is included in T.Phys-Manipulation
T.Malfunction of [ST-EAC SAC] is included in T.Malfunction of [SMG-IC].
T.Counterfeit is specific to [ST-EAC SAC] and do no conflict with the threats of [SMG-IC]

We can therefore conclude that the threats of [ST-EAC SAC] and [SMG-IC] are consistent.

4.5.2 Compatibility between OSP of [ST-EAC SAC] and [SMG-IC]

P.Manufact is included in P.Process-TOE.

P.Sensitive_Data, P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Terminal, P.Sensitive_Data, P.Active_Auth and P.Personalisation are specific to the MRTD and they do no conflict with the OSP of [SMG-IC].

We can therefore conclude that the OSP of [ST-EAC SAC] and [SMG-IC] are consistent.

4.5.3 Compatibility between assumptions of [ST-EAC SAC] and [SMG-IC]

A.Passive_Auth and A.Auth_PKI are included in A.Process-Sec-IC

A.Insp_Sys, is an assumptions specific to [ST-EAC SAC] and do no conflict with the assumptions of [SMG-IC].

We can therefore conclude that the assumptions for the environment of [ST-EAC SAC] and [SMG-IC] are consistent.

5. SECURITY OBJECTIVES

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

5.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.Data_Integrity Integrity of Data
The TOE must ensure integrity of the User Data and the TSF-data[13] 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.

OT.Data_Authenticity Authenticity of Data
The TOE must ensure authenticity of the User Data and the TSF-data[14] stored on it by enabling verification of their authenticity at the terminal-side[15].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)[16].

OT.Data_Confidentiality Confidentiality of Data
The TOE must ensure confidentiality of the User Data and the TSF-data[17] 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.

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.

Application note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)[18] cannot be achieved by the current TOE.

OT.Prot_Abuse_Func Protection against Abuse of Functionality

[13] where appropriate, see Table 3 above
[14] where appropriate, see Table 3 above
[15] verification of SO_D
[16] secure messaging after the PACE authentication, see also [ICAO-TR-SAC]
[17] where appropriate, see Table 3 above
[18] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [PKI] '.

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.

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,
- 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.

OT.Prot_Phys_Tamper Protection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's 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 electrical charges (using tools used in solid-state physics research and IC failure analysis),
- manipulation of the hardware and its security functionality, 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 functionality.

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.

The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment*.

OT.Identification Identification of the TOE

The TOE must provide means to store Initialisation[19] 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).

OT.AC_Pers Access Control for Personalisation 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 [PKI] 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.

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.

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 Version 1 as defined in [TR-EAC-1]. 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.

OT.Active_Auth_Proof Proof of MRTD's chip authenticity through AA

The TOE must support the General 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-9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

[19] amongst other, IC Identification data

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Travel document Issuer as the general responsible

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

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.

Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment:

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 (C_{CSCA}). 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 [PKI]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [PKI]. 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.

OE.Personalisation Personalisation 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 [PKI][20], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [PKI] (in the role of a DS).

Terminal operator: Terminal's receiving branch

OE.Terminal Terminal operating

The terminal operators must operate their terminals as follows:

[20] see also [PKI] , sec. 10

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [PKI].

2.) The related terminals implement the terminal parts of the PACE protocol [ICAO-TR-SAC], of the Passive Authentication [ICAO-TR-SAC] (by verification of the signature of the Document Security Object) and use them in this order[21]. The PACE terminal uses 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.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) 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, [PKI]).

5.) 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 according to the current PP.

Travel document holder Obligations

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.

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.

OE.Active_Auth_Verif Verification by Active Authentication
In addition to the verification by passive authentication, the inspection systems may use the verification by active authentication, which offers a stronger guaranty of the authenticity of the MRTD.

The following security objectives for the operational environment are additions to [PP-MRTD-SAC]:

Issuing State or Organisation

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

[21] This order is commensurate with [ICAO-TR-SAC].

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 additionally to those from [PP-MRTD-SAC] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this security target and not in [PP-MRTD-SAC].

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 additionally to those from [PP-MRTD-SAC] 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 one of the additional features of the TOE described only in this security target and not in [PP-MRTD-SAC].

Receiving State or Organisation

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

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 [4] and/or the Basic Access Control [6]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Justification: This security objective for the operational environment is needed additionally to those from [PP-MRTD-SAC] 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 also repeats partly the requirements from OE.Terminal in [PP-MRTD-SAC] and therefore also counters T.Forgery and A.Passive_Auth from [PP-MRTD-SAC]. This is done because a new type of Inspection System is introduced in this PP as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control.

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 Version 1.

Justification: This security objective for the operational environment is needed additionally to those from [PP-MRTD-SAC] 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.

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 additionally to those from [PP-MRTD-SAC] 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.

5.3 SECURITY OBJECTIVE RATIONALE

5.3.1 Rationale between objectives and threats, assumptions, OSP

The following table provides an overview for security objectives coverage.
Table and following explanations are copied from [PP-MRTD-EACV2]. Only the shaded parts are added.

Threats and assumptions included from the claimed PACE-PP [PP-MRTD-SAC] are marked *in italic letters.*[22]

	OT.Sens_Data_Conf	*OT.Chip_Auth_Proof*	*OT.AC_Pers*[23]	*OT.Data_Integrity*	*OT.Data_Authenticity*	*OT.Data_Confidentiality*	*OT.Tracing*	*OT.Prot_Abuse-Func*	*OT.Prot_Inf_Leak*	*OT.Identification*	*OT.Prot_Phys-Tamper*	*OT.Prot_Malfuntion*	OT.Active_Auth_Proof	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	*OE.Personalisation*	*OE.Passive_Auth_Sign*	*OE.Terminal*	*OE.Travel_Document_Holder*	*OE.Legislative_Compliance*	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Read_Sensitive_Data	X														X			X							
T.Counterfeit		X												X		X									
T.Skimming[24]				X	X	X																X			
T.Eavesdropping						X																			
T.Tracing							X															X			
T.Abuse-Func								X																	

[22] The rational comes from the [PP-MRTD-SAC] and it is not reproduced below.
[23] The Objectives marked *in italic letters* are included from the claimed [PP-MRTD-SAC]. They are listed for the complete overview of the security objectives.

[24] Threats and assumptions included from the claimed [PP-MRTD-SAC] are marked *in italic letters.* They are listed for the complete overview of threats and assumptions.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers[23]	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OT.Active_Auth_Proof	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative_Compliance	OE.Active_Auth_Sign	OE.Active_Auth_Verif
T.Information_Leakage									X																
T.Phys-Tamper											X														
T.Malfunction												X													
T.Forgery			X	X	X			X			X					X			X	X	X				
P.Sensitive_Data	X														X			X							
P.Personalisation			X							X									X						
P.Manufact										X															
P.Pre-Operational			X							X									X				X		
P.Terminal																X					X				
P.Card_PKI																				X					
P.Trustworthy_PKI																				X					
P.Active_Auth													X											X	X
A.Insp_Sys																X	X								
A.Auth_PKI															X			X							
A.Passive_Auth																X				X					

Table 5: Security Objective Rationale

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.

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”.

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 [7]. **OE.Exam_Travel_Document** enforces the terminals to perform the terminal part of the PACE protocol.

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 AA as specified in **OT.Active_Auth_Proof**.

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 Version 1 to verify the authenticity of the travel document’s chip.

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 [7] 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.

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 Version 1 to verify the Authenticity of the presented travel document’s chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** “Protection of data from the logical travel document” require the Inspection System to protect the logical travel document data during the transmission and the internal handling.

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 [7] 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”.

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.

5.3.2 Compatibility between objectives of [ST-EAC SAC] and [SMG-IC]

5.3.2.1 Compatibility between objectives for the TOE

O.Data_Conf, OT.Chip_Auth_Proof and OT.Active_Auth_Proof are supported by O.RND

OT.Data_Int is included in O.Phys-Manipulation.

OT.AC_Pers, is specific to [ST-EAC SAC] and it does no conflict with the objectives of [SMG-IC].
OT.Identification is included in O.Identification and supported by O.RND
OT.Prot_Abuse-Func is included in O.Abuse-Func.
OT.Prot_Inf_Leak is included in O.Leak-Forced and supported by O.RND
OT.Prot_Phys-Tamper is included in O.Phys-Manipulation and supported by O.RND
OT.Prot_Malfunction is included in O.Malfunction.

We can therefore conclude that the objectives for the TOE of [ST-EAC SAC] and [SMG-IC] are consistent.

5.3.2.2 Compatibility between objectives for the environment

OE.Personalisation is included in OE.Process-Sec-IC and supported by OE.Loader_Usage of [SMG-IC].

OE.Active_Auth_Sign and OE.Active_Auth_Verif are included in OE.TOE_Auth of [SMG-IC].

OE.Auth_Key_Travel_Document, OE.Authoriz_Sens_Data, OE.Exam_Travel_Document, OE.Prot_Logical_Travel_Document, OE.Ext_Insp_Systems, OE.Terminal, OE.Travel_Document_Holder, OE.Legislative_Compliance, OE.Passive_Auth_Verif are specific to [ST-EAC SAC] and they do no conflict with the objectives of [SMG-IC].

We can therefore conclude that the objectives for the environment of [ST-EAC SAC] and [SMG-IC] are consistent.

5.3.3 Justifications for adding objectives on the environment

5.3.3.1 Additions to [PP-MRTD-EACV2]

The only additional objectives on the environment are OE.Active_Auth_Sign and OE.Active_Auth_Verif. These objectives request the environment to support Active Authentication. AA is an operation outside [PP-MRTD-EACV2]. Therefore the added objectives on the environment do not weaken the TOE.

6. EXTENDED COMPONENTS DEFINITION

This security target uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0002]; others are defined in the protection profile [PP-MRTD-EACV2].

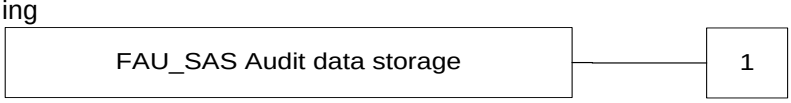
6.1 DEFINITION OF THE FAMILY FAU_SAS

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

FAU_SAS Audit data storage

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

Component levelling



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.

6.2 DEFINITION OF THE FAMILY FCS_RND

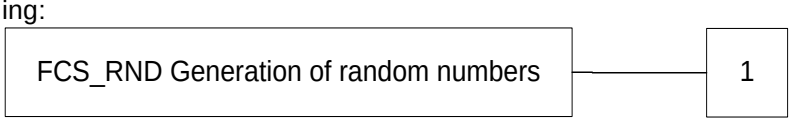
To define the IT security functional requirements of the TOE a sensitive family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation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

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 levelling:



FCS_RND.1 Generation of random numbers requires that 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*].

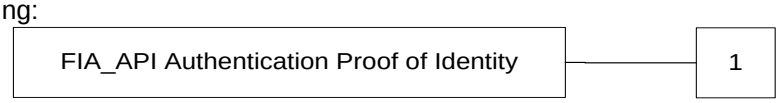
6.3 DEFINITION OF THE FAMILY FIA_API

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.

FIA_API Authentication Proof of Identity

Family behaviour
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 levelling:



FIA_API.1 Authentication 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*].

6.4 DEFINITION OF THE FAMILY FMT_LIM

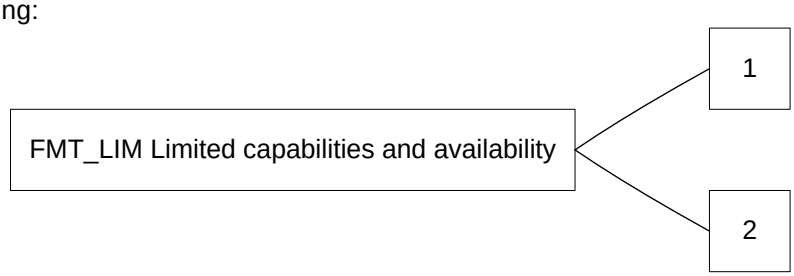
The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class 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.

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

FMT_LIM Limited capabilities and availability

Family behavior
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 requires that the TSF is built to provide only the capabilities (perform action, gather information) 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 life-cycle.

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.

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.

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].

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

(i) 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

(ii) 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.

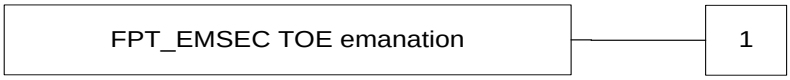
6.5 DEFINITION OF THE FAMILY FPT_EMS

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 part 2 [CC-2].

The family “TOE Emanation (FPT_EMS)” is specified as follows.

Family behaviour
This family defines requirements to mitigate intelligible emanations.

Component levelling:



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*].

7. SECURITY REQUIREMENTS

The definition of the subjects “Manufacturer”, “Pre-personalizer”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 2.4.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 10 “Glossary and acronyms” or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC-2]. The operation “load” is synonymous to “import” used in [CC-2].

Definition of security attributes:

security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR-EAC-1], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-EAC-1], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-EAC-1], A.5.1)

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

Name	Data
Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA 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 (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR-EAC-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key

Name	Data
	(PKCVCA) 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 (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) 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 (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (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 (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD'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. a Basic 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 MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Application note 20: 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 MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

7.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.
Refinements in this section are in underline font when the SFR's refinement is already present in [PP-MRTD-EACV2], and in bold font when the refinement is done in this ST. When the SFR is refined in the [PP-MRTD-EACV2] and additionally refined in this ST then the font is bold and underline.

For this section, a presentation choice has been selected. Each SFR present a table with different type of algorithms treated. For each case, there is no distinction regarding the technical objectives fulfilled by each row on the table (thus algorithm family). The technical objectives are the same disregarding this differentiation.

7.1.1 Class FAU Security Audit

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 with the capability to store the IC Identification Data in the audit records.

7.1.2 Class Cryptographic Support (FCS)

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

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_COP.1/PACE_ENC** and **FCS_COP.1/PACE_MAC**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_CKM.1.1 /DH_PACE

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as in **Table 6 algorithm column** and specified cryptographic key sizes as in **Table 6 column Key size** that meet the following: **Table 6 standard column**.

Algorithm type	algorithm	Key size	standard
/SKPICC	**ECDH Key Agreement Algorithm – [IEEE-P1363]**	**160, 192, 224, 256, 320, 384, 512, and 521 bits**	***[TR-03111]*** **]**
/TDESsession-ECDH	**ECDH Key Agreement Algorithm – 160, 192, 224, 256, 320, 384, 512, and 521 bits**	**112 bits**	***[TR-03111]*** **]**
/AESsession-ECDH	**ECDH Key Agreement Algorithm – 160, 192, 224, 256, 320, 384, 512, and 521 bits**	**128, 192, 256**	***[TR-03111]*** **]**

Table 6: FCS_CKM.1/DH_PACE iteration explanation

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]]: fulfilled by **FCS_COP.1/CA_ENC**, **FCS_COP.1/CA_MAC** and **FCS_COP.1/PACE_CAM**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**

FCS_CKM.1.1 /CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as in **Table 7 algorithm column** and specified cryptographic key sizes as in **Table 7 Key size column** that meet the following: **Table 7 standard column standard**.

Algorithm type	algorithm	Key size	standard
/TDESsession-DH	**DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits**	**112 bits**	**Diffie-Hellman key derivation protocol compliant to [PKCS#3]**
/AESsession-DH	**DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits**	**128, 192, and 256 bits**	***Diffie-Hellman key derivation protocol compliant to [PKCS#3]***
/TDESsession-ECDH	**ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, 512 and 521 bits**	**112 bits**	**[TR-EAC-1] , based on an ECDH protocol compliant to [TR-ECC]**
/AESsession-ECDH	**ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, 512 and 521 bits**	**128, 192, and 256 bits**	**[TR-EAC-1] , based on an ECDH protocol compliant to [TR-ECC]**

Table 7: FCS_CKM.1/CA iteration explanation

FCS_CKM.1/KeyPair Cryptographic key generation for AA and CA Key Pair

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: fulfilled by **FCS_COP.1/AA**, **FCS_COP.1/CA_MAC**, **FCS_COP.1/CA_ENC** and **FCS_COP.1/PACE_CAM**
FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note

FCS_CKM.1.1 /KeyPair | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as in **Table 8 algorithm column** and specified cryptographic key sizes as in **Table 8 Key size column** that meet the following: **Table 8 standard column.**

Algorithm type	algorithm	Key size	standard
/RSA	**RSA CRT Key generation**	**1024, 1280, 1536 and 2048 bits**	**none (generation of random numbers and Miller- Rabin primality testing)**
/ECC	**ECC Key generation**	**160, 192, 224, 256, 320, 384, 512 and 521 bits**	***FIPS 186-3 Appendix B.4.1***
CA/DH	**DH key generation**	**1024, 1280, 1536 and 2048 bits**	**ANSI X9.42**
CA/ECDH	**ECDH Key generation**	**160, 192, 224, 256, 320, 384, 512 and 521 bits**	**[IEEE-P1363]**

Table 8: FCS_CKM.1/KeyPair iteration explanation

Application notes:

- The dependency of FCS_CKM1/KeyPair on FCS_COP.1 is partly fulfilled by FCS_COP.1/CA_MAC and FCS_COP.1/CA_ENC. This dependence is not direct: FCS_CKM1/KeyPair generates a static key which in turn generate session keys, via FCS_CKM1/CA. These session keys then use FCS_COP.1/CA_MAC and FCS_COP.1/CA_ENC.
- The dependency of FCS_CKM1/KeyPair on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

FCS_CKM.1/PERSO Cryptographic key generation for Session keys

Hierarchical to: No other components
Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: fulfilled by **FCS_COP.1/PERSO**
FCS_CKM.4 Cryptographic key destruction]: fulfilled by **FCS_CKM.4**

FCS_CKM.1.1 /PERSO | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as in **Table 9 algorithm column** and specified cryptographic key sizes as in **Table 9 Key size column** that meet the following: **Table 9 standard column**.

Algorithm type	algorithm	Key size	standard
/TDES	**TDES ISK key derivation**	**112 bits**	**[ICAO-9303] normative appendix 5**
/GP	**GP session keys**	**112, 128 bits (and 192 & 256 bits for SCP03)**	**[GP211] SCP01, SCP02, or SCP03**

Table 9: FCS_CKM.1/PERSO iteration explanation

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]: fulfilled by **FCS_CKM.1/DH_PACE**, **FCS_CKM.1/CA**, and **FCS_CKM.1/PERSO**.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Secure erasing of the value** that meets the following: **None**.

Application note: Secure erasing of data is performed by overwriting the data with random numbers.

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]: fulfilled by **FCS_CKM.1/DH_PACE**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /PACE_ENC The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **Table 10 algorithm** and cryptographic key sizes **Table 10 Key size** that meet the following: **Table 10 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/ENC_TDES	**TDES in CBC mode**	**112 bits**	**ISO 10116**
/ENC_AES	**AES in CBC mode**	**128, 192, 256**	**ISO 10116**

Table 10: FCS_COP.1/PACE_ENC iteration explanation

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]: fulfilled by **FCS_CKM.1/DH_PACE**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /PACE_MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **Table 11 algorithm** and cryptographic key sizes **Table 11 Key size** that meet the following: **Table 11 standard column**.

Algorithm type	algorithm	Key size	List of standards
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 11: FCS_COP.1/PACE_MAC iteration explanation

FCS_COP.1/PACE_CAM Cryptographic operation – Modular Multiplication

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1 Cryptographic key generation]: fulfilled by **FCS_CKM.1/DH_PACE**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /PACE_CAM: The TSF shall perform modular multiplication with specify cryptography algorithm as in **Table 12 algorithm column** and cryptographic key sizes as in **Table 12 Key size** that meet the following: **Table 12 standards column**.

Algorithm type	algorithm	Key size	standards
/CAM_ECDH	**ECC**	**160, 192, 224, 256, 320, 384, 512, 521**	**[TR-ECC] ECKA - DH**

Table 12: FCS_COP.1/PACE_CAM iteration explanation

FCS_COP.1/CA_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]: fulfilled by **FCS_CKM.1/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /CA_ENC: The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **Table 13 algorithm** and cryptographic key sizes **Table 13 Key size** that meet the following: **Table 13 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/ENC_TDES	**TDES in CBC mode**	**112 bits**	**ISO 10116**
/ENC_AES	**AES in CBC mode**	**128, 192, 256**	**ISO 10116**

Table 13: FCS_COP.1/CA_ENC iteration explanation

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]: fulfilled by **FCS_CKM.1/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /SIG_VER: The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **Table 14 algorithm** and cryptographic key sizes **Table 14 Key size** that meet the following: **Table 14 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/RSA_VER	**RSA (STD)**	**1024, 1280, 1536, 2048, 3072, and 4096**	**RSA SHA PKCS#1** **RSA SHA PKCS#1 PSS**
/ECC_VER	**ECC**	**160, 192, 224, 256, 320, 384, 512, 521**	**[TR-ECC] ECDSA SHA**

Table 14: FCS_COP.1/SIG_VER iteration explanation

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]: fulfilled by **FCS_CKM.1/CA**
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /CA_MAC: The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **Table 15 algorithm** and cryptographic key sizes **Table 15 Key size** that meet the following: **Table 15 list of standards**.

Algorithm type	algorithm	Key size	List of standards
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 15: FCS_COP.1/CA_MAC iteration explanation

FCS_COP.1/PERSO Cryptographic operation – Symmetric encryption, decryption, and MAC during manufacturing

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/PERSO**.
FCS_CKM.4 Cryptographic key destruction: fulfilled by **FCS_CKM.4**.

FCS_COP.1.1 /PERSO: The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **Table 16 algorithm** and cryptographic key sizes **Table 16 Key size** that meet the following: **Table 16 List of standards**.

Algorithm type	algorithm	Key size	List of standards
/ENC_TDES	**TDES encryption and decryption**	**112 bits**	**[SP 800-67]**
/ENC_AES	**AES encryption and decryption**	**128, 192, 256**	**[FIPS 197]**
/MAC_TDES	**TDES Retail MAC**	**112 bits**	**ISO 9797-1**
/MAC_AES	**AES CMAC**	**128, 192, 256**	**[NIST-800-38B]**

Table 16: FCS_COP.1/ PERSO iteration explanation

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
FCS_CKM.1 Cryptographic key generation]: fulfilled by **FCS_CKM.1/KeyPair**
FCS_CKM.4 Cryptographic key destruction: not fulfilled, see application note.

FCS_COP.1.1 /AA: The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **Table 17 algorithm** and cryptographic key sizes **Table 17 Key size** that meet the following: **Table 17 List of standards**.

Algorithm type	algorithm	Key size	List of standards
/AA_RSA	**RSA**	**1024, 1280, 1536, 2048, 3072, and 4096 bits**	**ISO9796-2**
/AA_ECDSA	**ECDSA**	**160, 192, 224, 256, 320, 384, 512 and 521**	**[TR-ECC]**

Table 17: FCS_COP.1/AA iteration explanation

Application note:
- The dependency of FCS_COP.1/AA on FCS_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

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 **RGS [RGS-B1], [AIS20/31] and [SP 800-90] with seed entropy at least 128 bits**.

Application note: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

7.1.3 Class FIA Identification and Authentication

Table 18 provides an overview on the authentication mechanisms used.

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

Table 18: Overview on authentication SFR

Note the Chip Authentication Protocol Version 1 as defined in this protection profile includes

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

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

FIA_AFL.1/PERSO Authentication failure handling during pre-personalization and personalization phases

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by **FIA_UAU.1/PACE**
FIA_AFL.1.1 /Perso	The TSF shall detect when **Number in Table 19** unsuccessful authentication attempts occurs related to **Authentication type in Table 19**.
FIA_AFL.1.2 /Perso	When the defined number of unsuccessful authentication attempts has been met, the TSF shall **Actions in Table 19**.

Authentication type	Number	Actions
GP	**3**	**Block GP authentication**.
ISK key	**3**	**Block ISK Key**.

Table 19: FIA_AFL.1/PERSO iteration explanation

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 [**Number in Table 20**] 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, the TSF shall [**Actions in Table 20**].

Password	Number	Actions
MRZ, CAN	**1**	**Exponentially increase time delay before new authentication attempt is possible**.
PIN	**3**	**Block PIN**.

Table 20: FIA_AFL.1/PACE iteration explanation

FIA_UID.1/PERSO Timing of identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 /PERSO	The TSF shall allow **1. to establish a communication channel,** **2. to carry out the mutual authentication Protocol according to [GP]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 /PERSO	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/PERSO Timing of authentication

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification: fulfilled by **FIA_UID.1/PERSO**
FIA_UAU.1.1 /PERSO	The TSF shall allow **1. to establish a communication channel,** **2. to carry out the mutual authentication Protocol according to [GP]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 /PERSO	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

- FIA_AFL.1/PERSO, FIA_UID.1/PERSO, and FIA_UID.1/PERSO are extensions to [PP-MRTD-EACV2], in order to deal with identification and authentication in pre-personalisation and personalisation phases.

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-SAC],
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-EAC-1]
5. to carry out the Terminal Authentication Protocol v.1 according to [TR-EAC-1]

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

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

Application note: The SFR FIA_UID.1/PACE in the current ST covers the definition in [PP-MRTD-SAC] and extends it by EAC aspects 4 & 5. This extension does not conflict with the strict conformance to PACE PP.

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-SAC],
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-EAC-1]
6. to carry out the Terminal Authentication Protocol v.1 according to [TR-EAC-1]

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

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

Application note: The SFR FIA_UAU.1/PACE in the current ST covers the definition in [PP-MRTD-SAC] and extends it by EAC aspects 5 & 6. This extension does not conflict with the strict conformance to PACE PP.

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-SAC],
2. Authentication Mechanism based on **Triple-DES, AES**
3. Terminal Authentication Protocol v.1 according to [TR-EAC-1]

Application note: The authentication mechanisms use a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt.

Application note: The SFR FIA_UAU.4/PACE in the current ST covers the definition in [PP-MRTD-SAC] and extends it by EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP.

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-SAC],
2. Passive Authentication according to [ICAO-9303]
3. Secure messaging in MAC-ENC according to [ICAO-TR-SAC],
4. Symmetric Authentication Mechanism based on **Triple-DES, AES**
5. Terminal Authentication Protocol v.1 according to [TR-EAC-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. **TOE accepts the authentication attempt as Pre-personalization Agent by the Symmetric Authentication Mechanism with the Pre-personalization Agent Key.**
2. 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.
3. The TOE accepts the authentication attempt as Personalization Agent by **the Symmetric Authentication Mechanism with Personalization Agent Key**.
4. 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 v.1.
5. 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.

Application note: The SFR FIA_UAU.5.1/PACE in the current ST covers the definition in [PP-MRTD-SAC]and extends it by EAC aspect 5. The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in [PP-MRTD-SAC] and extends it by EAC aspects 4 and 5. These extensions do not conflict with the strict conformance to PACE PP.

FIA_UAU.6/PACE Re-authenticating – 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 PACE Protocol shall be verified as being sent by the PACE terminal.

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

Hierarchical to: No other components
Dependencies: No dependencies

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

FIA_API.1/CA Authentication Proof of Identity – Chip Authentication

Hierarchical to: No other components
Dependencies: No dependencies

FIA_API.1.1/CA The TSF shall provide a Chip Authentication Protocol v.1 according to [TR-EAC-1] to prove the identity of the TOE.

Application note: This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [TR-EAC-1]. 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], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1/AA Authentication Proof of Identity – Active Authentication

Hierarchical to: No other components
Dependencies: No dependencies

FIA_API.1.1/AA The TSF shall provide an **Active Authentication Protocol according to [ICAO-9303]** to prove the identity of the **TOE**.

Application note: This SFR requires the TOE to implement the Active Authentication Mechanism specified in [ICAO-9303]. The terminal generates a challenge then verifies whether the MRTD's chip was able or not to sign it properly using its Active Authentication private key corresponding to the Active Authentication public key (EF.DG15).

7.1.4 Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

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 on terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD.

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

FDP_ACF.1/TRM Security attribute based access control

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control; fulfilled by **FDP_ACC.1/TRM**
FMT_MSA.3 Static attribute initialization

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

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

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-SAC],after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

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

1. Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2. Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.
4. Any terminal being not successfully authenticated as Extended Inspection System with

the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.

5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4

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. ephemeral private key ephem - SK_{PICC}- PACE (by having generated a DH shared secret *K*).

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1/TRM Basic data exchange confidentiality

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

The TOE shall meet the requirement “Data exchange integrity (FDP_UIT.1)” as specified below (Common Criteria Part 2).

FDP_UIT.1/TRM Data exchange integrity

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]: fulfilled by **FDP_ACC.1/TRM** [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]: fulfilled by **FTP_ITC.1/PACE**

FDP_UIT.1.1 /TRM The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion,

/TRM insertion and replay has occurred.

Rationale for Refinement: Note that the Access Control SFP (cf. FDP_ACF.1.2) allows the Extended Inspection System (as of [ICAO-9303] and [PP-MRTD-BAC]) to access the data EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. Nevertheless there is explicitly no rule for preventing access to these data. More over their data integrity (cf. FDP_UIT.1) and confidentiality (cf. FDP_UCT.1) is ensured by the BAC mechanism being addressed and covered by [PP-MRTD-BAC]. The fact that the BAC mechanism is not part of the ST in hand is addressed by the refinement "after Chip Authentication".

7.1.5 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 ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and the Terminal.

7.1.6 Class FMT Security Management

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

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

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.

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (Common Criteria Part 2).

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. Personalization Agent,
3. Terminal,
4. PACE authenticated BIS-PACE

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

Application note: The MRTD also maintains the role Basic Inspection System due to a direct consequence of P.BAC-PP resp. OE.BAC-PP. Nevertheless this role is not explicitly listed in FMT_SMR.1.1, above since the TSF cannot maintain the role with respect to the assumed high attack potential due to the known weaknesses of the Document Basic Access Keys.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components
Dependencies: FMT_LIM.2 Limited capabilities: fulfilled by **FMT_LIM.2**.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:
Deploying test features after TOE delivery do not allow
1.User Data to be manipulated and disclosed,
2.TSF data to b e manipulated or disclosed,
3.software to be reconstructed,
4.substantial information about construction of TSF to be gathered which may enable other attacks.

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

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

Application note: The term “software” in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (Common Criteria Part 2). 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 the Initialization Data and Pre-personalization Data to the Manufacturer.

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

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 the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent

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 the 1. initial Country Verifying Certification Authority Public Key, 2. initial Country Verifying Certification Authority Certificate, 3. initial Current Date to **the Personalization Agent**.

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

Hierarchical to:	No other components

Dependencies: FMT_SMF.1 Specification of management functions: 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 the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate

to Country Verifying Certification Authority.

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 the Current date to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System.

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 **create and load** the Chip Authentication Private Key to **the Personalization Agent**.

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

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

FMT_MTD.1.1/ AAK The TSF shall restrict the ability to **create and load** the Active Authentication Private Key to **the Personalization Agent**.

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 the Document Security Object (SO_D) to the Personalisation Agent.

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 the
1. PACE passwords
2. Document Basic Access Keys,
3. Chip Authentication Private Key,
4. **Active Authentication Private Key**
5. Personalization Agent Keys

to none.

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2):

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components
Dependencies: FMT_MTD.1 Management of TSF data: fulfilled by : fulfilled by **FMT_MTD.1/CVCA_INI**, **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 and the Access Control.

Refinement: The certificate chain is valid if and only if

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

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

(3) the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.

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

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

Application note: The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

7.1.7 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)"

together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “TOE Emanation (FPT_EMS.1)” as specified below (Common Criteria Part 2 extended):

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit **electromagnetic and current emissions** in excess of **intelligible threshold** 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. Personalization Agent Key(s)
5. Chip Authentication Private Key
6. **Active Authentication Key, EF.DG3 and EF.DG4**

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

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K MAC, PACE-KEnc),
3. the ephemeral private key ephem SK PICC-PACE,
4. Personalization Agent Key(s)
5. Chip Authentication Private Key
6. **Active Authentication Key**.

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

The TOE shall meet the requirement “Failure with preservation of secure state (FPT_FLS.1)” as specified below (Common Criteria Part 2).

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.

The TOE shall meet the requirement “TSF testing (FPT_TST.1)” as specified below (Common Criteria Part 2).

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 **Conditions under which self test should occur** to demonstrate the correct operation of the TSF at condition:

1. **During initial start-up**
2. **Periodically during normal operation**
3. **After cryptographic computation**
4. **Before any use or update of TSF data**

The description of the self test is the following (for each corresponding number):

1. **RNG live test, sensor test, FA detection, Integrity Check of NVM ES**
2. **RNG monitoring, FA detection**
3. **FA detection**
4. **FA detection, Integrity Check of related TSF data**

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

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

Table 21: FPT_TST refinements

The TOE shall meet the requirement “Resistance to physical attack (FPT_PHP.3)” as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components
Dependencies: No dependencies.

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

7.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

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

Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

7.3 SECURITY REQUIREMENTS RATIONALE

7.3.1 Security Functional Requirements Rationale

The rationale in this paragraph comes from [PP-MRTD-EACV2] §6.3.1. Additions due to Active Authentication and secure messaging in personalisation are shaded.

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
FAU_SAS.1			X				X						
FCS_CKM.1/DH_PACE				X	X	X							
FCS_CKM.1/CA	X	X	X	X	X	X							
FCS_CKM.1/KeyPair		X											X
FCS_CKM.1/PERSO	X			X	X	X							
FCS_CKM.4	X		X	X	X	X							
FCS_COP.1/PACE_ENC						X							
FCS_COP.1/PACE_MAC				X	X								
FCS_COP.1/CA_ENC	X	X	X	X		X							
FCS_COP.1/SIG_VER	X		X										
FCS_COP.1/CA_MAC	X	X	X	X									
FCS_COP.1/PACE_CAM	X			X	X								X
FCS_COP.1/PERSO	X			X	X	X							
FCS_COP.1/AA													X
FCS_RND.1	X		X	X	X	X							
FIA_AFL.1/PERSO	X			X	X	X							
FIA_AFL.1/PACE										X			
FIA_UID.1/PERSO	X			X	X	X							
FIA_UAU.1/PERSO	X			X	X	X							
FIA_UID.1/PACE	X		X	X	X	X							
FIA_UAU.1/PACE	X		X	X	X	X							
FIA_UAU.4/PACE	X		X	X	X	X							
FIA_UAU.5/PACE	X		X	X	X	X							
FIA_UAU.6/PACE				X	X	X							
FIA_UAU.6/EAC	X		X	X	X	X							
FIA_API.1/CA		X											
FIA_API.1/AA													X
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							
FTP_ITC.1/PACE				X	X	X				X			
FMT_SMF.1		X	X	X	X	X	X						
FMT_SMR.1/PACE		X	X	X	X	X	X						
FMT_LIM.1								X					
FMT_LIM.2								X					
FMT_MTD.1/INI_ENA			X				X						
FMT_MTD.1/INI_DIS			X				X						
FMT_MTD.1/CVCA_INI	X												
FMT_MTD.1/CVCA_UPD	X												
FMT_MTD.1/DATE	X												
FMT_MTD.1/CAPK	X	X		X									

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse_Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Active_Auth_Proof
FMT_MTD.1/AAK													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_FLS.1									X			X	
FPT_TST.1									X			X	
FPT_PHP.3				X					X		X		

Table 22: Security functional requirement rationale

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.

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 SO_D 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 (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.

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 SO_D 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 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 K_{MAC}).
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 (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.
The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

In pre-personalisation, the SFR FCS_CKM.1/PERSO and FCS_COP.1/PERSO ensure the integrity of data transfers after successful authentication of the pre-personalisation agent according to FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO.

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 resp. FCS_CKM.1/CA 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 SO_D 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.

In pre-personalisation, the SFR FCS_CKM.1/PERSO and FCS_COP.1/PERSO ensure the authenticity of data transfers after successful authentication of the pre-personalisation agent according to FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO.

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 resp. FCS_CKM.1/CA 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 K_{ENC}). 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 SO_D 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.
In pre-personalisation, the SFR FCS_CKM.1/PERSO and FCS_COP.1/PERSO ensure the confidentiality of data transfers after successful authentication of the pre-personalisation agent according to FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO.

The security objective **OT.Sens_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 (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.
The SFRs FIA_UID.1/PERSO and FIA_UAU.1/PERSO, with the support of FIA_AFL.1/PERSO, require the identification and authentication of the pre-personalisation agent.

The security objective **OT.Chip_Auth_Proof** “Proof of travel document’s chip authenticity” is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [5] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.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.

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.

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 SO_D is card-individual) – FTP_ITC.1/PACE.

The security objective **OT.Prot_Phys_Tamper** “Protection against Physical Tampering” is covered by the SFR FPT_PHP.3.

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.

The security objective **OT.Activ_Auth_Proof** “Proof of MRTD’s chip authenticity through AA” is covered by FIA_API.1/AA that proves the identity of the TOE. FCS_COP.1/AA provides the signature. FMT_MTD.1/AAK and FMT_MTD.1/KEY_READ participate to confidentiality of AA private key.

7.3.2 Dependency Rationale

The rationale in this paragraph comes from [PP-MRTD-EACV2] §6.3.2. Additions due to Active Authentication are shaded.

SFR	Dependencies	Support of the dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/DH_PACE	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/PACE_ENC**, **FCS_COP.1/PACE_MAC** **FCS_CKM.4**
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/CA_ENC**, **FCS_COP.1/CA_MAC**, **FCS_COP.1/PACE_MAC**, **FCS_CKM.4**
FCS_CKM.1/KeyPair	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/CA_ENC**, **FCS_COP.1/CA_MAC**, **FCS_COP.1/PACE_MAC**, Not fulfilled, see note 1
FCS_CKM.1/PERSO	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	**FCS_COP.1/PERSO**, **FCS_CKM.4**
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1]	**FCS_CKM.1/DH_PACE**, **FCS_CKM.1/CA**, **FCS_CKM.1/PERSO**

SFR	Dependencies	Support of the dependencies
FCS_COP.1/PACE_ENC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/DH_PACE** **FCS_CKM.4**
FCS_COP.1/PACE_MAC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/DH_PACE** **FCS_CKM.4**
FCS_COP.1/PACE_CAM	FCS_CKM.1 FCS_CKM.4	**FCS_CKM.1/DH_PACE** **FCS_CKM.4**
FCS_COP.1/CA_ENC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/SIG_VER	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/CA_MAC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/CA** **FCS_CKM.4**
FCS_COP.1/PERSO	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/PERSO** **FCS_CKM.4**
FCS_COP.1/AA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	**FCS_CKM.1/KeyPair** Not fulfilled: see note 1
FCS_RND.1	No dependencies	
FIA_AFL.1/PERSO	FIA_UAU.1	**FIA_UAU.1/PERSO**
FIA_AFL.1/PACE	FIA_UAU.1	**FIA_UAU.1/PACE**
FIA_UID.1/PERSO	No dependencies	
FIA_UAU.1/PERSO	FIA_UID.1	**FIA_UID.1/PERSO**
FIA_UID.1/PACE	No dependencies	
FIA_UAU.1/PACE	FIA_UID.1	**FIA_UID.1/PACE**
FIA_UAU.4/PACE	No dependencies	
FIA_UAU.5/PACE	No dependencies	
FIA_UAU.6/PACE	No dependencies	
FIA_UAU.6/EAC	No dependencies	
FIA_API.1/CA	No dependencies	
FIA_API.1/AA	No dependencies	
FDP_ACC.1/TRM	FDP_ACF.1	**FDP_ACF.1/TRM**
FDP_ACF.1/TRM	FDP_ACC.1, FMT_MSA.3	**FDP_ACC.1/TRM**, Not fulfilled: see note 2
FDP_RIP.1	No dependencies	
FDP_UCT.1/TRM	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	**FDP_ACC.1/TRM**, **FTP_ITC.1/PACE**
FDP_UIT.1/TRM	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1, or FTP_TRP.1]	**FDP_ACC.1/TRM**, **FTP_ITC.1/PACE**
FTP_ITC.1/PACE	No dependencies	
FMT_SMF.1	No dependencies	
FMT_SMR.1/PACE	FIA_UID.1	**FIA_UID.1/PACE**
FMT_LIM.1	FMT_LIM.2	**FMT_LIM.2**

SFR	Dependencies	Support of the dependencies
FMT_LIM.2	FMT_LIM.1	**FMT_LIM.1**
FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/CVCA_INI	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/DATE	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/CAPK	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/AAK	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/PA	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	**FMT_SMF.1**, **FMT_SMR.1/PACE**
FMT_MTD.3	FMT_MTD.1	**FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD**
FPT_EMS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.3	No dependencies	

Table 23: Security functional requirement dependencies

Notes:

1. The dependency between **FCS_COP.1/AA** and **FCS_CKM.4** is not fulfilled because the key is permanently stored on the card.
2. The access control TSF according to **FDP_ACF.1/TRM** uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

7.3.3 Security Assurance Requirements Rationale

EAL5 was chosen because it provides a high level of independently assured security in a planned development. It requires a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.
The selection of the component ALC_DVS.2 provides a higher assurance of the security of the MRTD's development and manufacturing especially for the secure handling of the MRTD's material.
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.

For these additional assurance components, all dependencies are met or exceeded in the EAL5 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL5)		
ALC_DVS.2	no dependencies	-
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.5
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

Table 24: SAR Dependencies

7.3.4 Security Requirements – Mutual support and internal consistency

Cf [PP-MRTD-EACV2] §6.3.4

7.3.5 Compatibility between SFR of [ST-EAC SAC] and [SMG-IC]

FAU_SAS.1 of [ST-EAC SAC] is included in FAU_SAS.1 of [SMG-IC].

FCS_RND.1 of [ST-EAC SAC] is supported by FCS_RNG.1/RGS_IC of [SMG-IC].

FPT_EMS.1 and FPT_PHP.3 of [ST-EAC SAC] are included in FPT_PHP.3 of [SMG-IC].

FPT_FLS.1 of [ST-EAC SAC] is included in FPT_FLS.1 of [SMG-IC].

FCS_COP.1/PACE_ENC, FCS_COP.1/PACE_MAC, FCS_COP.1/CA_ENC, FCS_COP.1/CA_MAC, FCS_COP.1/PERSO of [ST-EAC] are supported by FCS_COP.1/TDES and FCS_COP.1/AES of [SMG-IC].

FCS_CKM.4, FIA_AFL.1/PERSO, FIA_AFL.1/PACE, FIA_UID.1/PERSO, FIA_UID.1/PACE, FIA_UAU.1/PERSO, FIA_UAU.1/PACE, FIA_UAU.4/PACE, FIA_UAU.5/PACE, FIA_UAU.6/PACE, FIA_UAU.6/EAC, FIA_API.1/CA, FIA_API.1/AA, FDP_ACC.1/TRM, FDP_ACF.1/TRM, FDP_RIP.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1/PACE, FMT_LIM.1, FMT_LIM.2, all FMT_MTD.1, FMT_MTD.3,FPT_TST.1, FTP_ITC.1/PACE, FCS_COP.1/PACE_CAM, FCS_COP.1/SIG_VER, FCS_CKM.1/DH_PACE, FCS_CKM.1/CA, FCS_CKM.1/KeyPair, and FCS_CKM.1/PERSO are specific to [ST-EAC SAC] and they do not conflict with [SMG-IC].

We can therefore conclude that the SFR of [ST-EAC SAC] and [SMG-IC] are consistent.

8. TOE SUMMARY SPECIFICATION

8.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel v2.3 embedded software (including the optional NVM ES) and by the chip.

8.1.1 TSFs provided by the eTravel v2.3 (MultiApp v4.1) Software

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.CA	Chip Authentication
SF.TA_CER	Validity of the Certificate Chain
SF.TA_AUT	Terminal Authentication Mechanism
SF.AA	Active Authentication

Table 25: Security Functions provided by the MultiApp V4.1 Software

The SF.REL function provides the protection of data on the TOE. It encompasses:

- physical protection of the TOE as defined in **FPT_PHP.3**, **FPT_EMS.1**, **FPT_FLS.1**,

the test mechanisms as defined in

FPT_TST.1,

- protection against misuse of tests as defined in **FMT_LIM.1** and **FMT_LIM.2**,

The SF.AC function provides the access control of the TOE. It encompasses:

- the access control by the terminal as defined in **FDP_ACC.1/TRM** and **FDP_ACF.1/TRM**,
- the access control to specific data as defined in **FAU_SAS.1**, **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/AAK**, **FMT_MTD.1/PA**, and **FMT_MTD.1/KEY_READ**,
- the role management as defined in **FMT_SMR.1/PACE** ,
- the management functions linked to the different states of the TOE as defined in **FMT_SMF.1**.

The SF.SYM_AUTH function provides the symmetric authentication functions to the TOE. It encompasses:

- the PACE identification and authentication as defined in **FIA_AFL.1/PACE**, **FIA_UID.1/PACE**, **FIA_UAU.1/PACE**, **FIA_UAU.4/PACE**, **FIA_UAU.5/PACE**, and **FIA_UAU.6/PACE**,
- the identification and authentication in personalisation phase as defined in **FIA_AFL.1/PERSO**, **FIA_UID.1/PERSO**, and **FIA_UAU.1/PERSO**,
- The role authentication as requested by **FMT_SMR.1/PACE .**

The SF.SM function provides the secure messaging of the TOE. It encompasses:

- the establishment of SM as defined in **FTP_ITC.1/PACE**,
- the secure transfer of data through SM as defined in **FDP_UCT.1/TRM** and **FDP_UIT.1/TRM**,
- the cryptographic mechanisms used for the authentication and the SM, as defined in **FCS_CKM.1/DH_PACE**, **FCS_CKM.1/PERSO**, **FCS_COP.1/PACE_ENC**, **FCS_COP.1/PACE_MAC**, **FCS_COP.1/PERSO**, and **FCS_RND.1**. Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function.
- the erasure of session keys as defined in **FCS_CKM.4** and **FDP_RIP.1**.

The SF.CA function provides the chip Authentication. It encompasses:

- the CA authentication as defined in **FIA_API.1/CA**, **FIA_UAU.6/EAC**
- the CA cryptographic algorithm as defined in **FCS_CKM.1/CA**, **FCS_COP.1/CA_ENC** and **FCS_COP.1/CA_MAC**,
- the generation and input of CA keys, as defined in **FCS_CKM.1/KeyPair** and **FMT_MTD.1/CAPK**,
- The role authentication as requested by **FMT_SMR.1/PACE .**

The SF.TA_CER function provides the validity of the Certificate Chain. It encompasses:

- the initialisation and update of data used for the validation, as defined in **FMT_MTD.1/CVCA_INI**, **FMT_MTD.1/CVCA_UPD**, **FMT_MTD.1/DATE**, and **FMT_MTD.3**.

The SF.TA_AUT function provides the TA Mechanism. It encompasses:

- the cryptographic mechanisms used for the authentication, as defined in **FCS_COP.1/SIG_VER**,
- The role authentication as requested by **FMT_SMR.1/PACE .**

The SF.AA function provides the active authentication. It encompasses:

- the AA protocol itself as defined in **FIA_API.1/AA**,
- the AA cryptographic algorithm as defined in **FCS_COP.1/AA**,
- the generation and input of AA keys, as defined in **FCS_CKM.1/KeyPair** and **FMT_MTD.1/AAK**.

8.1.2 TSFs provided by the Samsung S3FT9MH

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC]. The IC and its primary embedded software have been evaluated at level EAL 6+.

SF	Description
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 26: Security Functions provided by the Samsung S3FT9MH

These SF are described in [SMG-IC].

9. GLOSSARY AND ACRONYMS

Glossary

Term	Definition
Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
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.
Application note	Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the evaluation or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data.
Authenticity	Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer
Basic Access Control (BAC)	Security mechanism defined in [PKI] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS.
Basic Inspection System with Basic Access Control protocol (BIS-BAC)	A technical system being used by an official organisation[25] and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn form printed MRZ data for reading the less-sensitive data (travel document details data and biographical data) stored on the travel document. See also par. 1.2.5; also [PKI].
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority[26] 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. A technical system being used by an inspecting authority and verifying the ePass presenter as the ePass holder (for ePassport: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass holder). The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol.
Biographical data (biodata)	The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data.
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).
Card Access Number (CAN)	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport),

[25] an inspecting authority; concretely, by a control officer
[26] concretely, by a control officer

Term	Definition
	semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [ICAO-TR-SAC]
Counterfeit	An unauthorised copy or reproduction of a genuine security document made by whatever means [PKI].
Country Signing CertA Certificate (CCSCA)	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority and stored in the rightful terminals.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePasss 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. [PKI], 5.5.1.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data transmitted between the TOE and an inspection system using BAC [PKI]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [PKI].
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 RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the ePassport application (EF.SOD) of the travel document. It may carry the Document Signer Certificate (CDS); see [PKI], sec. A.10.4.
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS)(CDS), see [PKI]. This role is usually delegated to a Personalisation Agent.
Eavesdropper	A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document.
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; see [PKI].
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 [ICAO-TR-SAC].
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [PKI].
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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [PKI].
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

Term	Definition
	might be restricted to certain life cycle phases.
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 cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
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; see [PKI].
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; see [PKI].
Initialisation Data	Any data defined by the travel document manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as travel document material (IC identification data).
Inspection	The act of an official organisation (inspection authority) examining an travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [PKI].
Inspection system	see BIS-PACE for this PP. see also BIS-BAC for general information
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 stored upon have not been altered from that created by the travel document Issuer.
Issuing Organisation	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [PKI].
Issuing State	The country issuing the travel document; see [PKI].
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [PKI]. The capacity expansion technology used is the travel document's chip.
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; see [PKI]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
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; see [PKI].
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 phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
PACE password	A password needed for PACE authentication, e.g. CAN or MRZ.
PACE Terminal (PCT)	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. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ).
Passive authentication	Security mechanism implementing (i) verification of the digital signature of the Card/Chip or Document Security Object and (ii) comparing the hash values of

Term	Definition
	the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [PKI].
Passport (physical and electronic)	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [ICAO-TR-SAC]. 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.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document.
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 [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (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 Card/Chip Security Object, if installed, and 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.
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.
Receiving State	The Country to which the travel document holder is applying for entry; see [PKI].
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 [ISO14443]
Rightful equipment (rightful terminal or	A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up

Term	Definition
rightful Card)	to the respective root CertA. A rightful terminal can be either BIS-PACE (see Inspection System).
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [PKI].
Secure messaging in combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
Skimming	Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-SAC], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.
Supplemental Access Control	A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.
Terminal	A Terminal is any technical system communicating with the TOE through a contactless / contact interface.
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 [PKI] (there "Machine readable travel document").
Travel document (electronic)	The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
Travel document holder	A person for whom the ePass Issuer has personalised the travel document.
Travel document Issuer (issuing authority)	Organisation authorised to issue an electronic Passport to the travel document holder
Travel document presenter	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC-1]).
Unpersonalised travel document	travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip.
User Data	All data (being not authentication data) (i)stored in the context of the ePassport application of the travel document as defined in [PKI]and (ii)being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]). CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
AA	Active Authentication
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [9])
BIS-PACE	Basic Inspection System with PACE
CAN	Card Access Number
CC	Common Criteria
CertA	Certification Authority
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
RF	Radio Frequency
SAC	Supplemental Access Control
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure, see [ICAO-TR-SAC]
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE Security Policy (defined by the current document)