cv act ePasslet/EACv2-SAC v1.8

Security Target

BSI-DSZ-CC-0799

Common Criteria / ISO 15408

EAL 4+

Document Version 1.04 • 2012-08-16

cv cryptovision GmbH • Munscheidstr. 14 • 45886 Gelsenkirchen • Germany
www.cryptovision.com • info@cryptovision.com • +49-209-167-2450

Content

Version Control

Version	Date	Author	Changes to Previous Version
0.1	2011-03-13	Thomas Zeggel	Initial version based on Protection Profile "Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control", Version 1.0, 21 September 2010.
0.2	2011-03-15	Thomas Zeggel	Completed version including all parts. Minor questions and comments marked for further discussions.
0.3	2011-03-16	Benjamin Drisch, Thomas Zeggel	Small changes and corrections. Some questions open for discussion with NXP.
0.4	2011-05-11	Benjamin Drisch, Thomas Zeggel	Small changes after discussion with TÜViT
0.5	2011-08-26	Benjamin Drisch	Changes from TÜViT review of BAC-ST included
0.6	2011-08-30	Benjamin Drisch, Thomas Zeggel	Small corrections
0.7	2011-09-20	Thomas Zeggel	Changes according to TüvIT observation report dated 2011-09-12.
0.8	2011-10-13	Thomas Zeggel	Integration of iterated cryptographic SFRs into one with an „or" connection.
0.9	2011-11-10	Benjamin Drisch, Thomas Zeggel	Changes according to the results of the BSI evaluation kick-off meeting and the TüvIT observation report to the SSCD ST; additional change of SFR FIA_AFL.1. Platforms corrected (no P5Cx080).
0.95	2012-02-06	Thomas Zeggel	Changed reference in table 1. Changed product name in ePasslet/EACv2-SAC v1.8. Comments in SFR mappings of chapter 2.2 added. Change of name of chapter 1.1. Reference [ZertIC080] corrected. Certificates of Crypto Libs referenced. Additional references in chapters 1.1, 1.2 and 1.3.2. Names of hardware platforms corrected. Key lengths adjusted according to latest JCOP ST.
0.96	2012-02-16	Benjamin Drisch	Changes based on remarks from TUEViT OR
0.97	2012-02-21	Benjamin Drisch	Changes due to remarks from BSI: • Added certification ID of platform and involved application in section 1.3.2
0.98	2012-02-23	Benjamin Drisch	Changes due to further remarks from BSI: • Added certification ID of crypto lib and hardware in section 1.3.2 • Further concretized applications involved in actual TOE in different mask variants in section 1.3.2 • Added version and exact reference for PACE as well as remarks about EC parameters from JCOP to FIA_UAU.4, FIA_UAU.5 and FIA_AFL.1 FCS • Included remark on PP conformance claim in section 2.1
0.99	2012-02-27	Thomas Zeggel	Small correction in the version control description; missing reference [JCOP_UGM] added.

1.0	2012-03-06	Benjamin Drisch	Changes due to further remarks from BSI: • Remark about fixed configuration and exclusion of code loading concretized in section 1.3.1 • Further concretized applications involved in actual TOE in section 1.3.2 • Added remark about random number generation being provided by the underlying JCOP platform (section 6.1.2.4) • Renamed FCS_CKM.1.1/3DES to FCS_CKM.1.1 • Changed SHA reference to FIPS 180-4 • Annotated FCS_COP.1/Auth to comment on the mis-leading use of “decryption” in this context
1.01	2012-03-09	Benjamin Drisch	Changes due to further remarks from BSI: • Replaced reference for FIPS 180-4 with FIPS 180-4 • Clarified PP-0056 reference in 3.1.1.1
1.02	2012-03-15	Benjamin Drisch	• Added remark about MIFARE not being part of the security functionality claimed by this Security Target • Clarified life cycle of the TOE according to ALC
1.03	2012-04-16	Benjamin Drisch	• Clarified TOE definition and life-cycle description
1.04	2012-08-16	Benjamin Drisch	• Explicitely stated contact-based interface in TOE defini-tion (1.3.2) • Corrected reference to Guidance Manual

1 Introduction

1.1 ST/TOE Identification

Title:	cv act ePasslet/EACv2-SAC v1.8 Security Target
Version:	v1.04
Origin:	cv cryptovision GmbH
Compliant to:	Common Criteria Protection Profile – “Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control” (PP-MRTD-SAC/PACE V2) [PP-SAC]
Product identification:	cv act ePasslet/EACv2-SAC v1.8
ROM identification value:	P5Cx081UA: 8F80EC
Javacard OS platform:	[ZertJCOP081]
Cryptographic library:	[ZertCL081]
Security controller:	[ZertIC081]
TOE identification:	cv act ePasslet/EACv2-SAC v1.8
TOE documentation:	Administration and user guide [Guidance]

1.2 ST overview

The aim of this document is to describe the Security Target for MRTD chips based on the EACv2-SAC application of the cv act ePassslet Suite. The cv act ePasslet Suite is a set of Javacard applets intended to be used exclusively on the NXP JCOP Javacard OS platform, which is certified according to CC EAL 5+ [ZertJCOP081]. The cv act ePasslet Suite as well as the NXP JCOP operating system are provided within the ROM mask of a smart card chip based on the NXP P5CD security controller, which is itself certified according to CC EAL 5+ [ZertIC081], and a certified cryptographic library [ZertCL081].

This security target claims strict conformance to the Protection Profile “Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control” (PP-MRTD-SAC/PACE V2) [PP-SAC].

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 functionalities.

The assurance level for the TOE is CC EAL4+.

1.3 TOE overview

1.3.1 Overview of cv act ePasslet Suite

The cv act ePasslet Suite is a modular multi-application solution for eID documents based on Java Card.

It provides the following applications:

Application name	Function	Standard
cv act ePasslet/BAC	Basic Access Control	ICAO Doc 9303
cv act ePasslet/EACv1.11	Extended Access Control, V1.11	BSI TR03110, V1.11
cv act ePasslet/EACv2-SAC	Extended Access Control, V2.05	BSI TR03110, V2.05; ICAO-TR-SAC,
cv act ePasslet/GeID	German eID card	BSI TR03127, BSI TR03110
cv act ePasslet/ePKI	IAS with own PKCS#15 profile	PKCS#15
cv act ePasslet/IDL	International Driving License	ISO 18013
cv act ePasslet/eHIC	European Health Insurance	CWA 15974
cv act ePasslet/EuCCB	European Citizen Card - Base Profile	CEN/TS 15480
cv act ePasslet/EuCCF	European Citizen Card - French Profile	GIXEL IAS-ECC V1.01
cv act ePasslet/eVR	Electronic Vehicle Registration	EU Council Directive 1999/37/EC
cv act ePasslet/NIDS	Combination of EAC V1.11 and ePKI	BSI TR03110, V1.11, PKCS#15

Table 1: Customer view of the available applications in the cv act ePasslet Suite.

These applications are realized by configurations of one or more predefined applets; while each application has a distinct configuration, different applications might use the same underlying applet. For details on the relation between applets and applications please refer to Figure 1 below.

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. Multiple applications can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed below. A common combination could be an EACv1 applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application (offered as own standard product configuration “NIDS” as listed in Table 1, Figure 1 and Figure 2).

The product is available in two variants:

Variant 1

- available on P5Cx081 and P5Cx041
- covering all applications provided in Table 1
- certified products (on P5Cx081 only):
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - EACv2-SAC certified according to SAC/PACE-PP
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact and contactless with PACE)

The following Figure 1 gives an overview of the available applications and actual applets in variant 1.

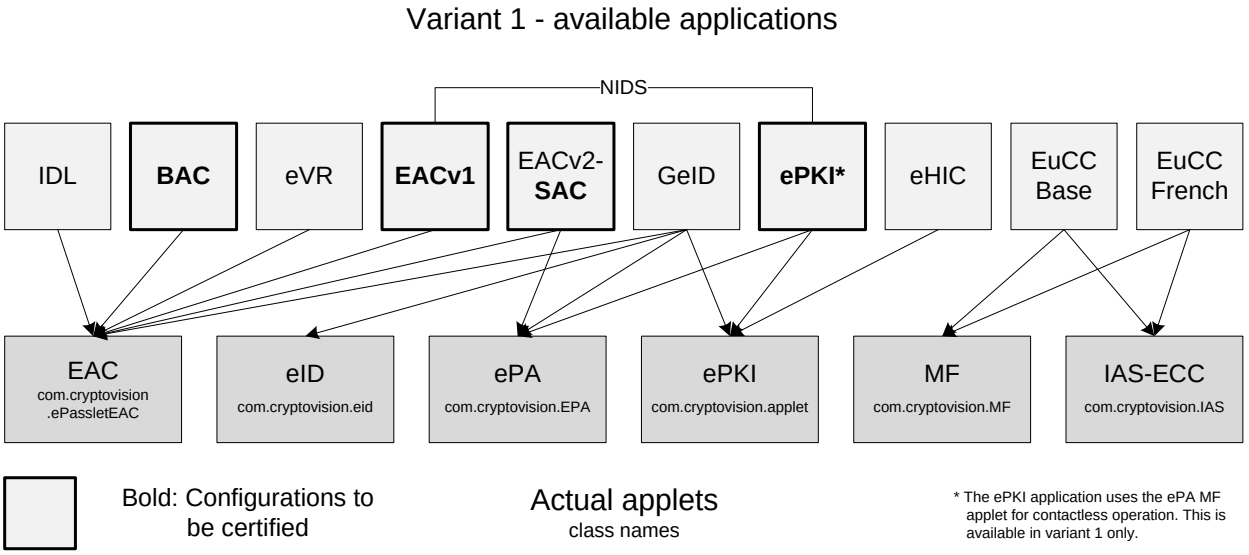


Figure 1: Available applications and actual applets in variant 1.

The other version (variant 2) contains a subset of these applications:

Variant 2

- available on P5Cx080 and P5Cx040
- Contains the applets and applications indicated in Figure 2
- certified products:
  - BAC certified according to PP0055
  - EACv1 certified according to PP0056
  - ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface only)

The following Figure 2 gives an overview of the available applications and actual applets in variant 2.

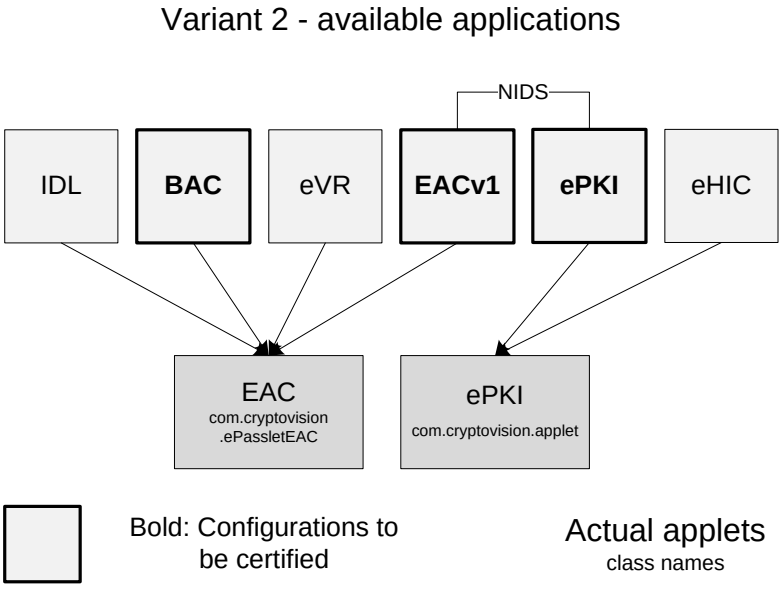


Figure 2: Available applications and actual applets in variant 2.

Combinations of certified and non-certified applications are possible (as long as these applications use one of the above applets instantiated from ROM).

Via configuration the instanciated applications can be tied to the contactless and/or the contact interface, respectively. BAC, EACv1, EACv2-SAC require exclusive access to the contactless interface. Hence, if one of these applications is used (in certified configuration), further (certified or non-certified) applications have to be bound to the contact interface.

The configuration of the TOE claimed by this Security Target is fixed after personalization. Additional applications can be instanciated as specified above from ROM only. This explicitly excludes additional applet code being loaded and installed into EEPROM.

1.3.2 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the cv act ePasslet/EACv2-SAC application it can be programmed according to the Logical Data Structure (LDS) [ICAODoc] and provides the Supplemental Access Control according to the ICAO document [ICAOTR].

The TOE consists of

- the circuitry of the MRTD's chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna,
- the platform with the Java Card operation system JCOP 2.4.1R3 by NXP, in the variant
    - JxA081, A, B1, B4, Certification ID BSI-DSZ-CC-0675-2011 ([ST_JCOP081], [ZertJCOP81]) with crypto library version 2.7, Certification ID BSI-DSZ-CC-0633-2010 ([ST_CL081], [ZertCL081]) and hardware P5Cx081V1A, Certification ID BSI-DSZ-CC-0555-2009 ([ST_IC081], [ZertIC081])
- cv act ePasslet/EACv2-SAC v1.8 as the only application that has access to the contactless interface,
- the associated guidance documentation Administrator and User Guidance [Guidance].

The TOE's functionality claimed by this Security Target is realized by the cv act ePasslet/EACv2-SAC application and is only available in variant 1 (refer to Figure 1 above) on P5Cx081.

Some of the underlying platform variants of this composite TOE provide MIFARE functionality; please note that this functionality is out of scope of the TOE's security functionality claimed by this Security Target.

1.3.3 TOE usage and security features for operational use

This paragraph is directly based on the corresponding paragraph in the protection profile [PP_SAC].

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this securety 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), (iii) the CAN for visual and machine reading using OCR methods on the data page and (iv) data elements on the MRTD's chip according to LDS for machine reading. The authentication of the traveler 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) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State or Organization 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 [ICAODoc] as specified by ICAO on the integrated circuit. It presents 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 optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both[1]
    (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) [ICAODoc]. 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 Access Control to the logical MRTD, Active Authentication of the MRTD's chip, and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAODoc]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment. The ICAO defines the advanced security method PACE V2 Access Control to the logical MRTD in [ICAOTR].

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 PACE V2 Access Control Mechanism. The PACE V2 Access Control Mechanism replaces the BAC Access Control Mechanism. It offers a higher security level as explained in [ICAOTR].This security target does not address the Active Authentication and the Extended Access Control. They are optional security mechanisms. The PACE V2 Access Control is a security feature which is mandatory in the TOE. The inspection system (i) reads optically the MRTD or the CAN, (ii) authenticates itself as inspection system by means of Document PACE V2 Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAOTR].

1.3.4 Major security features of the TOE

The TOE provides the following TOE security functionalities:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data.

[1] These additional biometric reference data are optional.

- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS (with the exception of the handling of the CMAC Sub-Keys for Secure Messaging and padding issues) and comprises the following primitives and key lengths:
  - hashing with SHA-1 and SHA-256
  - encryption and decryption with Triple-DES or AES and cryptographic key sizes 112 or 128, 192, 256 bit
  - Triple-DES or AES Retail-MAC and cryptographic key sizes of 112 or 128, 192, 256 bit
- TSF_SecureMessaging realizes a secure communication channel with MACs and encryption based on AES (128, 192 or 256 bit key length) or Triple-DES (112 bit key length).
- TSF_Auth_PACE-V2 realizes the PACE authentication mechanism (ECDH, key lengths between 128 and 320 bit).
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.
- TSF_OS contains all security functionalities provided by the certified platform (IC, crypto library, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform.

1.3.5 TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP0035], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.). This paragraph is directly based on the corresponding paragraph in the protection profile [PP_SAC].

1.3.5.1 Phase 1 “Development”

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

(Step 2) The software developer[2] 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.

The manufacturing documentation of the IC including the IC Dedicated Software and the IC Embedded Software (operating system) is securely delivered to the IC manufacturer. The IC Embedded Software to be loaded by the MRTD manufacturer, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

1.3.5.2 Phase 2 “Manufacturing”

(Step 3) In a first step, the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software loaded by the IC manufacturer. The IC manu-

[2] Please note that in this ST the role software developer of the protection profile is subdivided into two separate roles: the operating system is developed by the OS software developer, and the MRTD application by the (MRTD) software developer.

facturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The TOE delivery according to CC is the delivery of the IC (with the application code in ROM) from the IC manufacturer to the MRTD manufacturer.

(Step 4) The MRTD manufacturer combines the IC with hardware for the physical interface in the passport book.

(Step 5) The MRTD manufacturer (i) creates the MRTD application (instantiates the appropriate applet in the correct configuration) and (ii) equips MRTD's chips with pre-personalization Data.

PP application note 1: Creation of the application implies the Applet instantiation.

In this step the final (but not yet personalized) MRTD is generated from the certified components according to the binding initialization and pre-personalization guidelines provided in [Guidance].

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.

1.3.5.3 Phase 3 "Personalization of the MRTD"

(Step 6) 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. Note that the TSF data (data for the operation of the TOE upon which the enforcement of the SFR relies; cf. [CC_1] §97) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the PACE V2 Authentication Control Key. TSF data also include the source code.

The signing of the Document security object by the Document Signer [ICAODoc] 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.

PP application note 2: The TSF data (data for the operation of the TOE upon which the enforcement of the SFR relies; cf. [CC_1] §97) comprise (but are not limited to) the Personalization Agent Authentication Key(s) and the PACE V2 Authentication Control Key. TSF data also include the source code.

PP application note 3: As in the PP this ST distinguishes between the roles „personalization agent" and „doument signer"

1.3.5.4 Phase 4 "Operational Use"

(Step 7) The TOE is used as MRTD chip by the traveler 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 or Organization but they can never be modified.

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

PP application note 5: The intention of the underlying PP [PP-SAC] is to consider at least the phases 1 and parts of phase 2 (i.e. Step1 to Step3) as part of the evaluation and therefore to define the TOE delivery according to CC after Step 3 of this phase2. Since specific production steps of phase 2 are of minor security relevance (e. g. booklet manufacturing and antenna integration) these are not part of the CC evaluation

under ALC. Nevertheless the decision about this has to be taken by the certification body resp. the national body of the issuing State or Organization. In this case the national body of the issuing State or Organization is responsible for these specific production steps.

Note that the personalization process and its environment may depend on specific security needs of an issuing State or Organization. All production, generation and installation procedures after TOE delivery up to the “Operational Use” (phase 4) have to be considered in the product evaluation process under AGD assurance class.

Remark: This ST considers only phase 1 and parts of phase 2 (steps 1 - 3) as part of CC evaluation under ALC.

2 Conformance claims

2.1 CC conformance

This security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, version 3.1 revision 3, [CC_1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, July 2009, version 3.1 revision 3, [CC_2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, July 2009, version 3.1 revision 3, [CC_3],

as follows:

- Part 2 extended,
- Part 3 conformant,

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [CC_4]

has to be taken into account.

This security target claims strict conformance also to the Common Criteria Protection Profile – "MachineReadable Travel Document SAC (PACE V2) Supplemental Access Control" (PP-MRTD-SAC/PACE V2) [PP_SAC]. No extensions have been made.

This security target is conforming to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in CC part 3 [CC_3].

The evaluation of the TOE uses the result of the CC evaluation of the chip platform claiming conformance to the PP [PP0035]. The hardware part of the composite evaluation is covered by the certification report [ZertIC081]. In addition, the evaluation of the TOE uses the result of the CC evaluation of the crypto library and the JCOP Javacard OS claiming conformance to the PP [PP_Javacard]. The Javacard OS part of the composite evaluation is covered by the certification report [ZertJCOP081] , the crypto library by the certification report [ZertCL081].

2.2 Statement of Compatibility concerning Composite Security Target

2.2.1 Assessment of the Platform TSFs

The following Table 2 lists all Security Functionalities of the underlying Platform ST and shows, which Security Functionalities of the Platform ST are relevant for this Composite ST and which are irrelevant. The first column addresses specific Security Functionality of the underlying platform, which is assigned to Security Functionalities of the Composite ST in the second column. The last column provides additional information on the correspondence if necessary.

Relevant Platform TSF-group	Correspondence in this ST	References/Remarks
SF.AccessControl	TSF_Access	
SF.Audit	TSF_Admin	
SF.CryptoKey	TSF_Secret	
SF.CryptoOperation	TSF_Crypto	
SF.I&A	TSF_Access	
SF.SecureManagement	TSF_Admin, TSF_Integrity	
SF.Transaction	TSF_Integrity	
SF.Hardware	TSF_OS	Implicitly used via JCOP (TSF_OS)*
SF.CryptoLib	TSF_OS	Implicitly used via JCOP (TSF_OS)*

Table 2: Relevant platform TSF-groups and their correspondence

*** Remark:** The Platform TSF-groups "SF.Hardware" and "SF.CryptoLib" are not directly used by Security Functions of the TOE, they are (implicitly) invoked by calls to the JCOP operating system, though. These OS calls are grouped in the TSF_OS.

2.2.2 Assessment of the Platform SFRs

The following Table 3 provides an assessment of all relevant Platform SFRs.

Relevant Platform SFR	Correspondence in this ST	References/Remarks
FAU: Security Audit		
FAU_ARP.1/JCS	FPT_PHP.3	Internal counter for security violations complement JCOP mechanisms
FAU_SAA.1	FPT_PHP.3	Internal counter for security violations complement JCOP mechanisms
FAU_SAS.1	FAU_SAS.1	Fulfillment of the platform SFR leads directly to the SFR of this ST.
FCS: CRYPTOGRAPHIC SUPPORT		
FCS_CKM.1	FCS_CKM.1	The requirement in this ST is equivalent to parts of the platform ST.
FCS_CKM.2	No correspondence	Out of scope (managed within JCOP) No contradiction to this ST
FCS_CKM.3	No correspondence	Out of scope (managed within JCOP) No contradiction to this ST
FCS_CKM.4	FCS_CKM.4	The requirements are equivalent (physically overwriting the keys with zeros).
FCS_COP.1	FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC	The requirements are equivalent: FCS_COP.1/SHA of this ST corresponds to the platform SFR FCS_COP.1/SHA-1

Relevant Platform SFR	Correspondence in this ST	References/Remarks
		and FCS_COP.1/SHA256; FCS_COP.1/ENC and FCS_COP.1/AUTH correspond to the platform SFR FCS_COP.1/TDES_MRTD; FCS_COP.1/MAC corresponds to the platform SFR FCS_COP.1/MAC_MRTD for TDES and to FCS_COP.1/AES for AES.
FCS_RNG.1	FCS_RND.1	Fulfillment of the platform SFR leads directly to the SFR of this ST.
FDP: User Data Protection		
FDP_ACC.1/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FDP_ACC.1/SCP	No correspondence	Out of scope (JCOP memory management) No contradiction to this ST
FDP_ACC.2/FIREWALL	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FDP_ACF.1/FIREWALL	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ACF.1/CMGR	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ACF.1/SCP	No correspondence	Out of scope (JCOP access control mechanisms) No contradiction to this ST
FDP_ETC.1	No correspondence	Out of scope (JCOP data control mechanisms) No contradiction to this ST
FDP_IFC.1/JCVM	No correspondence	Out of scope (refers to Virtual Machine) No contradiction to this ST
FDP_IFC.1/SCP	No correspondence	No contradiction to this ST
FDP_IFF.1/JCVM	No correspondence	Out of scope (refers to Virtual Machine) No contradiction to this ST
FDP_ITC.1	No correspondence	Out of scope (JCOP data control mechanisms) No contradiction to this ST

Relevant Platform SFR	Correspondence in this ST	References/Remarks
FDP_ITT.1/SCP	No correspondence	Out of scope (platform internal data transfer) No contradiction to this ST
FDP_RIP.1	FCS_CKM.4	Relied on for key deletion No contradiction to this ST
FDP_ROL.1/FIREWALL	No correspondence	Out of scope (refers to Virtual Machine) No contradiction to this ST
FDP_SDI.2	No correspondence	Out of scope (JCOP internal data integrity protection) No contradiction to this ST
FIA: Identification and Authentication		
FIA_AFL.1/PIN	No correspondence	Out of scope (no PINs used within applet) No contradiction to this ST
FIA_AFL.1/CMGR	No correspondence	Out of scope (refers to card manager) No contradiction to this ST
FIA_ATD.1/AID	No correspondence	Out of scope (JCOP AID management) No contradiction to this ST
FIA_UAU.1	FIA_UAU.1	The SFR in this ST extends the allowed actions of the platform SFR. No contradiction to this ST.
FIA_UAU.3/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UAU.4/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UID.1/CMGR	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FIA_UID.2/AID	No correspondence	Out of scope (JCOP AID management) No contradiction to this ST
FIA_USB.1	No correspondence	Out of scope (JCOP applet management) No contradiction to this ST
FMT: Security Management		
FMT_LIM.1	FMT_LIM.1	The SFR of this St is refinement of the platform SFR. No contradictions to this ST.
FMT_LIM.2	FMT_LIM.2	The SFR of this St is refinement of the

Relevant Platform SFR	Correspondence in this ST	References/Remarks
		platform SFR. No contradictions to this ST.
FMT_MSA.1/JCRE	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.1/CMGR	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.2/JCRE	No correspondence	Out of scope (JCOP object handling) No contradiction to this ST
FMT_MSA.3/FIREWALL	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.3/CMGR	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MSA.3/SCP	No correspondence	Out of scope (JCOP firewall mechanism) No contradiction to this ST
FMT_MTD.1/JCRE	No correspondence	Out of scope (modyfing list of registered applets' AID). No contradiction to this ST
FMT_MTD.3	No correspondence	Out of scope (JCOP LF state handling) No contradiction to this ST
FMT_SMF.1	FMT_SMF.1	Fullfillment of the platform SFR is used for fulfillment of the SFR of this ST.
FMT_SMR.1/JCRE	No correspondence	Out of scope (JCOP specific roles) No contradiction to this ST
FMT_SMR.1/CMGR	No correspondence	Out of scope (JCOP specific roles) No contradiction to this ST
FPR: Privacy		
FPR_UNO.1	No correspondence	Out of scope (JCOP package separation) No contradiction to this ST
FPT: Protection of the TSF		
FPT_EMSEC.1	FPT_EMSEC.1	FPR_EMSEC.1.1 is equivalent, FPT_EMSEC.1.2 is more restricted in this ST. No contradiction.
FPT_FLS.1/JCS	FPT_FLS.1	Internal countermeasures for detecting security violations complement JCOP mechanisms

Relevant Platform SFR	Correspondence in this ST	References/Remarks
		No contradiction to this ST
FPT_FLS.1/SCP	FPT_FLS.1	Internal countermeasures for detecting security violations complement JCOP mechanisms
FPT_ITT.1/SCP	No correspondence	Out of scope (platform internal data transfer) No contradiction to this ST
FPT_PHP.1	No correspondence	Out of scope (hardware mechanism) No contradiction to this ST
FPT_PHP.3/SCP	FPT_PHP.3	The SFRs are identical.
FPT_RCV.3/SCP	No correspondence	No contradiction to this ST
FPT_RCV.4/SCP	No correspondence	No contradiction to this ST
FPT_TDC.1	No correspondence	Refers to LC state before Applet instantiation No contradiction to this ST
FPT_TST.1	FPT_TST.1	The SFR is equivalent. No contradiction to the ST.
FRU: Resource Utilisation		
FRU_FLT.2/SCP	No correspondence	Out of scope (JCOP internal) No contradiction to this ST
FTP: Trusted Path/Channels		
FTP_ITC.1/CMGR	No correspondence	Out of scope (JCOP internal) No contradiction to this ST

Table 3: Relevant platform SFRs and their correspondence

2.2.3 Assessment of the Platform Objectives

The following table provides an assessment of all relevant Platform objectives.

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
O.PROTECT_DATA	OT.Data_Int, OT.Data_Conf	
O.SIDE_CHANNEL	OT.Prot_Inf_Leak	
O.OS_DECEIVE	No correspondence	
O.FAULT_PROTECT	OT.Prot_Malfunction	
O.PHYSICAL	OT.Prot_Phys-Tamper	
O.IDENTIFICATION	OT.Identification	
O.RND	No correspondence	Out of scope No contradiction to this ST
O.SID	No correspondence	Out of scope No contradiction to this ST

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
O.MF_FW	No correspondence	Out of scope No contradiction to this ST
O.OPERATE	No correspondence	Out of scope No contradiction to this ST
O.RESOURCES	No correspondence	Out of scope No contradiction to this ST
O.FIREWALL	No correspondence	Out of scope No contradiction to this ST
O.REALLOCATION	No correspondence	Out of scope No contradiction to this ST
O.SHRD_VAR_CONFID	No correspondence	Out of scope No contradiction to this ST
O.SHRD_VAR_INTEG	No correspondence	Out of scope No contradiction to this ST
O.ALARM	No correspondence	Out of scope No contradiction to this ST
O.TRANSACTION	No correspondence	Out of scope No contradiction to this ST
O.CIPHER	No correspondence	Out of scope No contradiction to this ST
O.PIN-MNGT	No correspondence	Out of scope No contradiction to this ST
O.KEY-MNGT	No correspondence	Out of scope No contradiction to this ST
O.CARD-MANAGEMENT	No correspondence	Out of scope No contradiction to this ST
O.SCP.RECOVERY	No correspondence	Out of scope No contradiction to this ST
O.SCP.SUPPORT	No correspondence	Out of scope No contradiction to this ST
O.SCP.IC	No correspondence	Out of scope No contradiction to this ST

Table 4: Relevant platform objectives and their correspondence

2.2.4 Assessment of Platform Threats

The following Table 5 provides an assessment of all relevant Platform objectives.

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks

Relevant Platform Oberctive	Correspondence in this ST	References/Remarks
T.ACCESS_DATA	T.Eavesdropping	
T.OS_OPERATE	No correspondence	Out of scope No contradiction to this ST
T.OS_DECEIVE	No correspondence	Out of scope No contradiction to this ST
T.LEAKAGE	T.Information_Leakage	
T.FAULT	T.Malfunction	
T.RND	No correspondence	Out of scope No contradiction to this ST
T.PHYSICAL	T.Phys-Tamper	
T.CONFID-JCSCODE	No correspondence	Out of scope No contradiction to this ST
T.CONFIDAPPLI-DATA	T.Information_Leakage	
T.CONFID-JCSDATA	No correspondence	Out of scope No contradiction to this ST
T.INTEG-APPLICODE	No correspondence	Out of scope No contradiction to this ST
T.INTEG-JCSCODE	No correspondence	Out of scope No contradiction to this ST
T.INTEG-APPLIDATA	T.Forgery	
T.INTEG-JCSDATA	No correspondence	Out of scope No contradiction to this ST
T.SID.1	No correspondence	Out of scope No contradiction to this ST
T.SID.2	No correspondence	Out of scope No contradiction to this ST
T.EXE-CODE.1	No correspondence	Out of scope No contradiction to this ST
T.EXE-CODE.2	No correspondence	Out of scope No contradiction to this ST
T.RESOURCES	No correspondence	Out of scope No contradiction to this ST

Table 5: Relevant platform thretas and their correspondence

2.2.5 Assessment of Platform Organisational Security Policies

The platform ST contains only the Organisational Security Policy “OSP.PROCESS-TOE” referring to accurate identification of each TOE instance. This policy will be fulfilled by a distinct product code for the platform and for the composite TOE each. This policy does not contradict to the policies of this ST.

2.2.6 Assessment of Platform Operational Environment

2.2.6.1 Assessment of Platform Assumptions

In the first column, the following table lists all significant assumptions of the Platform ST. The last column provides an explanation of relevance for the Composite TOE.

Significant Platform Assumption	Relevance for Composite ST
A.USE_DIAG	A.USE_DIAG is required in the Platform ST to cover secure communication. There is no corresponding assumption in the Composite ST. Secure communication is enforced by TSF_Access and hence supports this assumption directly.

Table 6: Significant assumptions of the Platform ST.

2.2.6.2 Assessment of Platform Security Objectives and SFRs for the Operational Environment

There are no significant Platform Security Objectives and no Platform SFRs for the Operational Environment to be considered.

3 Security problem definition

3.1 Introduction

3.1.1 Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

3.1.1.1 Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [ICAODoc]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

The TOE described in this security target specifies only the PACE V2 mechanisms with resistance against high attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM.

The TOE prevents read access to sensitive User Data

- Sensitive biometric reference data (EF.DG3, EF.DG4), which can be accessed under EAC protection (cf. [PP0056])[3].

A sensitive item is the following more general one.

3.1.1.2 Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

3.1.2 Subjects

This security target considers the following subjects:

3.1.2.1 Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

3.1.2.2 Personalization Agent

[3] This reference to the Protection Profile BSI-PP-0056, version 1.10, 25th March 2009 has been taken from the underlying Protection Profile and does not refer to the current BSI-PP-0056-V2.

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [ICAODoc].

3.1.2.3 Terminal

A terminal is any technical system communicating with the TOE through the interface.

3.1.2.4 Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

- The **Basic Inspection System** (BIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the BAC Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the BAC Access Control by optical reading the MRTD or other parts of the passport book providing this information.
- The **Supplemental Inspection System** (SIS) (i) contains a terminal for the communication with the MRTD's chip, (ii) implements the terminals part of the PACE V2 Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the PACE V2 Access Control by optical reading the MRTD or other parts of the passport book providing this information.
- The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.
- The **Extended Inspection System** (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

PP application note 6: This security target does not distinguish between the SIS, GIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.

3.1.2.5 MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

3.1.2.6 Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

3.1.2.7 Attacker

A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

PP Application note 7: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.2 Assumptions

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

3.2.1 A.MRTD_Manufact MRTD manufacturing on steps 4 to 6

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

3.2.2 A.MRTD_Delivery MRTD delivery during steps 4 to 6

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

- Procedures shall ensure protection of TOE material/information under delivery and storage.
- Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
- Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

3.2.3 A.Pers_Agent Personalization of the MRTD's chip in step 6

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document PACE V2 Access Keys, derived from the MRZ or the CAN, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

3.2.4 A.Insp_Sys Inspection Systems for global interoperability during step 7

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Supplemental Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the PACE V2 Access Control [ICAOTR]. The Supplemental Inspection System reads the logical MRTD under PACE V2 Access Control and performs the Passive Authentication to verify the logical MRTD.

PP application note 8: According to [ICADoc] the support of the Passive Authentication mechanism is mandatory whereas the PACE V2 Access Control is optional. This Security Target does not address Primary Inspection Systems therefore the PACE V2, which replaces BAC is mandatory within this PP.

3.3 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.

3.3.1 T.Chip_ID Identification of MRTD's chip

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the communication interface. The attacker cannot read and does not know the MRZ data, nor the CAN printed on the MRTD data page in advance.

3.3.2 T.Skimming Skimming the logical MRTD

An attacker imitates the inspection system to read the logical MRTD or parts of it via the communication channel of the TOE. The attacker cannot read and does not know the MRZ data, nor the CAN printed on the MRTD data page in advance.

3.3.3 T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data, or the CAN printed on the MRTD data page but the attacker does not know these data in advance.

Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data, nor the CAN printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

3.3.4 T.Forgery Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another chip.

3.3.5 T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational environment after delivery to MRTD holder.

The TOE shall avert the threats as specified below.

3.3.6 T.Information_Leakage Information Leakage from MRTD's chip

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

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 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 the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

3.3.7 T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose confidential TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) 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 direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and 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.

3.3.8 T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

3.4 Organizational security policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1 [CC_1], section A.6.3).

3.4.1 P.Manufact Manufacturing of the MRTD's chip

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

3.4.2 P.Personalization Personalization of the MRTD by issuing State or Organization only

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

3.4.3 P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the PACE V2 Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document PACE V2 Access Keys as defined in [ICAOTR].

PP application note 9: The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAODoc].Note, that EF.DG3 and EF.DG4 are only readable after successful EAC authentication not being covered by this security target.

4 Security objectives

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

4.1 Security Objectives for the TOE

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

4.1.1 OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAODoc] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

PP Application note 10: The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordingly. The support for adding data in the “Operational Use” phase is optional.

4.1.2 OT.Data_Int Integrity of personal data

The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

4.1.3 OT.Data_Conf Confidentiality of sensitive biometric reference data

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Supplemental Inspection System. The Supplemental Inspection System shall authenticate itself by means of the PACE V2 Access Control based on knowledge of the Document PACE V2 Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Supplemental Inspection System.

4.1.4 OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s). In Phase 4 “Operational Use” the TOE shall identify itself only to a successful authenticated Supplemental Inspection System or Personalization Agent.

PP application note 11: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identifica-

tion Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 “Operational Use” the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the interface before successful authentication as Supplemental Inspection System or as Personalization Agent.

In a multi-applicative product, data allowing to identify the IC or the MRTD, might be disclosed by other applications. This will be prevented within the other applications, though.

4.1.5 OT.Prot_Abuse-Func Protection against Abuse of Functionality

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

4.1.6 OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD’s chip

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

PP application note 12: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

4.1.7 OT.Prot_Phys-Tamper Protection against Physical Tampering

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

4.1.8 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 has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application note 13: 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 objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for the Operational Environment

4.2.1 Issuing State or Organization

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

4.2.1.1 OE.MRTD_Manufact Protection of the MRTD Manufacturing

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

4.2.1.2 OE.MRTD_ Delivery Protection of the MRTD delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
    - origin and shipment details,
    - reception, reception acknowledgement,
    - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

4.2.1.3 OE.Personalization Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger

image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

4.2.1.4 OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAODoc].

4.2.2 Receiving State or Organization

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

4.2.2.1 OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Supplemental Inspection System (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the PACE V2 Access Control [ICAOTR].

4.2.2.2 OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

4.2.2.3 OE.Prot_Logical_MRTD Protection of data from the logical MRTD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under PACE V2 Access Control will use inspection systems which implement the terminal part of the PACE V2 Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Supplemental Inspection Systems).

4.3 Security Objective Rationale

The following table provides an overview for security objectives coverage.

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Absue-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				X											
T.Skimming			X												
T.Eavesdropping			X												
T.Forgery	X	X					X					X	X	X	
T.Abuse-Func					X						X				
T.Information_Leakage						X									
T.Phys-Tamper							X								
T.Malfunction								X							
P.Manufact				X											
P.Personalization	X			X							X				
P.Personal_Data		X	X												
A.MRTD_Manufact									X						
A.MRTD_Delivery										X					
A.Pers_Agent											X				
A.Insp_Sys													X		X

Table 7: Security Objective Rationale

For the detailed description of the rationale the reader is referred to the protection profile [PP_SAC].

5 Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [PP0002], other components are defined in this security target.

5.1 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.

5.1.1 FAU_SAS Audit data storage

Family behavior

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

Component leveling

FAU_SAS Audit data storage	1

FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1
	There are no management activities foreseen.
Audit:	FAU_SAS.1
	There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: authorized users] with the capability to store [assignment: list of audit information] in the audit records.

5.2 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.

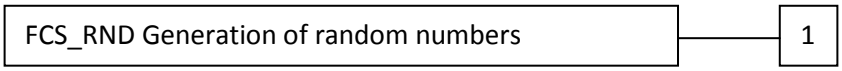
The family “Generation of random numbers (FCS_RND)” is specified as follows.

5.2.1 FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS_RND.1	Generation of random numbers requires that 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].

5.3 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.

5.3.1 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].

PP application note 14: 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 ist 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.

5.4 Definition of the Family FPT_EMSEC

The sensitive family FPT_EMSEC (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].a

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

Family behavior

This family defines requirements to mitigate intelligible emanations.

Component leveling:

FCS_EMSEC TOE emanation	1

FPT_EMSEC.1	TOE emanation has two constituents:
FPT_EMSEC.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMSEC.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMSEC.1
	There are no management activities foreseen.
Audit:	FPT_EMSEC.1
	There are no actions defined to be auditable.
FPT_EMSEC.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit [assignment: types of emissions] in excess of the [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
FPT_EMSEC.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].

6 Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [CC_1] of the CC. Each of these operations is used in this ST and the underlying PP.

Operations already performed in the underlying PP [PP_SAC] are uniformly marked by ***bold italic*** font style; for further information on details of the operation, please refer to [PP_SAC].

Operations performed within this Security Target are marked by **bold underlined** font style; further information on details of the operation is provided in foot notes.

6.1 Security Functional Requirements for the TOE

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

6.1.1 Class Security Audit (FAU)

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

6.1.1.1 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.

PP application note 15: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

6.1.2 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.

6.1.2.1 FCS_CKM.1 Cryptographic key generation – Generation of Document V2 Session Keys by the TOE

6.1.2.1.1 FCS_CKM.1

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Triple-DES or AES**[4] and specified cryptographic

[4] [assignment: cryptographic key generation algorithm]

key sizes sizes **112 bit or 128, 192, 256 bit**[5] that meet the following: ***[ICAOTR], normative appendix 5***.[6]

PP application note 16: The TOE is equipped with the Document PACE V2 Access Key generated and downloaded by the Personalization Agent. The PACE V2 Access Control Authentication Protocol described in [ICAOTR], produces agreed parameters to generate the ENC and the MAC session keys for secure messaging. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1.

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

6.1.2.2 FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physically overwriting the keys with zeros**[7] that meets the following: **none**[8].

PP application note 17: The TOE shall destroy the encryption key and the MAC message authentication keys for secure messaging.

6.1.2.3 FCS_COP.1 Cryptographic operation

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

6.1.2.3.1 FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA	The TSF shall perform ***hashing*** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256**[9] and cryptographic key sizes ***none*** that meet the following: **FIPS 180-4 [FIPS180-4]**[10].

[5] [assignment: cryptographic key sizes]

[6] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[7] [assignment: cryptographic key destruction]

[8] [assignment: list of standards]

[9] [selection: SHA or other approved algorithms]

[10] [selection: FIPS 180-2 or other approved standards]]

PP application note 18: This SFR requires the TOE to implement the hash function for the cryptographic primitive of the PACE V2 Access Control Authentication Mechanism (see also FIA_UAU.4).

6.1.2.3.2 FCS_COP.1/ENC Cryptographic operation – Encryption / Decryption

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ENC	The TSF shall ***perform secure messaging (PACE V2) – encryption and decryption*** in accordance with a specified cryptographic algorithm **Triple-DES or AES**[11] and cryptographic key sizes **112 or 128, 192, 256 bit**[12] that meet the following: **FIPS 46-3 [FIPS46-3] or FIPS 197 [FIPS197], respectively**[13].[14]

PP application note 19: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the PACE V2 Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4. See also [ICAOTR].

6.1.2.3.3 FCS_COP.1/AUTH Cryptographic operation – 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] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AUTH	The TSF shall perform ***symmetric authentication – encryption and decryption*** in accordance with a specified cryptographic algorithm **Triple-DES or AES**[15] and cryptographic key sizes **112 or 128, 192, 256] bit**[16] that meet the following: **FIPS 46-3 [FIPS46-3] or FIPS 197 [FIPS197], respectively**[17].[18]

PP application note 20: This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

Remark:** This SFR refers to the implicit authentication by derivation of a symmetric key from a password and subsequent encryption of a random nonce in the first step of the PACE protocol. As such the description in the PP "The TSF shall perform ***symmetric authentication – encryption AND

[11] [assignment: cryptographic algorithm]

[12] [assignment: cryptographic key sizes]

[13] [assignment: list of standards]

[14] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[15] [assignment: cryptographic algorithm]

[16] [assignment: cryptographic key sizes]

[17] [assignment: list of standards]

[18] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

***DECRYPTION**" is misleading and should read „"The TSF shall perform **symmetric authentication**" as there is no decryption process involved.*

6.1.2.3.4 FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/MAC	The TSF shall perform ***secure messaging – message authentication code*** in accordance with a specified cryptographic algorithm **Triple-DES CBC (Retail-MAC) or AES CMAC**[19] and cryptographic key sizes of **112 or 128, 192, 256 bit**[20] that meet the following **ISO 9797-1 [ISO9797-1] or SP 800-38b [SP800-38b], respectively**[21].[22]

PP application note 21: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the PACE V2 Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4. The authorized cryptographic algorithms and key sizes are specified in [ICAOTR].

6.1.2.4 FCS_RND.1 Random Number Generation

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

6.1.2.4.1 FCS_RND.1 Quality metric for random numbers

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet **the AIS 20 Class K3 quality metric**[23].

PP application note 22: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

Application note: The random number generation is provided by the underlying JCOP platform.

6.1.3 Class Identification and Authentication (FIA)

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

6.1.3.1 FIA_UID.1 Timing of identification

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

[19] [assignment: cryptographic algorithm]

[20] [assignment: cryptographic key sizes]

[21] [assignment: list of standards]

[22] The combination of the two cryptographic algorithms with an „or" is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[23] [assignment: a defined quality metric]

FIA_UID.1.1 The TSF shall allow

1. ***to read the Initialization Data in Phase 2 "Manufacturing",***
2. ***to read the random identifier in Phase 3 "Personalization of the MRTD",***
3. ***to read the random identifier in Phase 4 "Operational Use"***

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

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

PP application note 23: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document PACE V2 Access Keys) the user role Supplemental Inspection System is created by writing the Document PACE V2 Access Keys. The Supplemental Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document PACE V2 Access Key to authenticate the user as Supplemental Inspection System.

PP application note 24: In the "Operational Use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Supplemental Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. *This identifier is randomly selected and does not violate the OT.Identification.*

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

6.1.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

1. ***to read the Initialization Data in Phase 2 "Manufacturing",***
2. ***to read the random identifier and the file CardAccess in Phase 3 "Personalization of the MRTD",***
3. ***to read the random identifier and the file CardAccess in Phase 4 "Operational Use"***

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

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

PP application note 25: The Supplemental Inspection System and the Personalization Agent authenticate themselves.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

6.1.3.3 FIA_UAU.4 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 The TSF shall prevent reuse of authentication data related to

1. ***PACE V2 Access Control Authentication Mechanism*,***
2. ***Authentication Mechanism based on Triple-DES or AES***[24].[25]

PP application note 26: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

PP application note 27: The PACE V2 Access Control Mechanism is a mutual device authentication mechanism defined in [20]. The last step of this mutual authentication may allow a unique identification of the MRTD's chip. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID.

***Remark:** PACE V2 refers to PACE version 2 with 224 – 320 bit according to BSI-TR-03110 [TR03110v2], section 4.2. For PACE operation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below (Common Criteria Part 2).

6.1.3.4 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide

1. ***PACE V2 Access Control Authentication Mechanism****
2. ***Symmetric Authentication Mechanism based on Triple-DES or AES***[26].[27]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user’s claimed identity according to ***the following rules***:

1. ***the TOE accepts the authentication attempt as Personalization Agent by the mechanism: Symmetric Authentication Mechanism with the Personalization Agent Key***[28].
2. ***the TOE accepts the authentication attempt as Supplemental Inspection System only by means of the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys***

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

[25] The combination of the two cryptographic algorithms with an „or“ is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

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

[27] The combination of the two cryptographic algorithms with an „or“ is due to the fact that the final TOE may be configured in a way that only one of the two cryptographic algorithms is activated.

[28] [selection : the PACE V2 Access Control Authentication Mechanism with the Personalization Agent Keys, the Symmetric Authentication Mechanism with the Personalization Agent Key, [assignment other]]

PP application note 28: The PACE V2 Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Supplemental Inspection System uses the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

***Remark:** PACE V2 refers to PACE version 2 with 224 – 320 bit according to BSI-TR-03110 [TR03110v2], section 4.2. For PACE operation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

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

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions: Failure of MAC verification in a command received by the TOE.

The TOE shall meet the requirement "Authentication failure handling (FIA_AFL.1)" as specified below (Common Criteria Part 2).

PP application note 29: The PACE V2 Access Control Mechanism specified in [ICAODoc] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated PACE V2 user.

PP application note 30: Note that in case the TOE should also fulfill [PP0056] the PACE V2 communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the PACE V2 based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the PACE V2 communication but are protected by a more secure communication channel established after a more advanced authentication process.

6.1.3.6 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when **one**[29] unsuccessful authentication attempt occurs related to **PACE V2 authentication* with a non-blocking password**[30].

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

[30] [assignment: list of authentication events]; note that the non-blocking password could be a MRZ, CAN or PUK.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**[31], the TSF shall **reject the authentication and wait for the next authentication attempt.**[32].

PP application note 31: <applied>

Application note: The assignment operation in FIA_AFL.1.2 reflects the fact that due to the implementation the authentication procedere consumes a defined minimal amount of time. Because the MRZ possesses enough entropy for this reaction time, this is sufficient even to prevent a brute force attack with attack potential beyond high. Since the CAN does not represent a secret, because it may be revealed already to external entities, there is no need to consider a brute force attack against the CAN. The calculation time for authentication is sufficient to prevent the skimming of the TOE even for a random 6 digit CAN value.

***Remark:** PACE V2 refers to PACE version 2 with 224 – 320 bit according to BSI-TR-03110 [TR03110v2], section 4.2. For PACE operation please also note the remark in the JCOP user guidance manual [JCOP_UGM], section 2.2.1 on EC domain parameters.

6.1.4 Class User Data Protection (FDP)

6.1.4.1 FDP_ACC.1 Subset access control

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

6.1.4.1.1 FDP_ACC.1 Subset access control – PACE V2 Access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the ***PACE V2 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***.

6.1.4.2 FDP_ACF.1 Security attribute based access control

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

6.1.4.2.1 FDP_ACF.1 Basic Security attribute based access control – PACE V2 Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the ***PACE V2 Access Control SFP*** to objects based on the following:

1. ***Subjects:***
   a. ***Personalization Agent,***
   b. ***Supplemental Inspection System,***
   c. ***Terminal,***

[31] [assignment: met or surpassed],

[32] [assignment: list of actions]

2. ***Objects:***
   a. ***data EF.DG1 to EF.DG16 of the logical MRTD,***
   b. ***data in EF.COM,***
   c. ***data in EF.SOD,***
3. ***Security attributes***
   a. ***authentication status of terminals.***

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. ***the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,***
2. ***the successfully authenticated Supplemental Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.***

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rule:

1. ***Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.***
2. ***Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD.***
3. ***The Supplemental Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.***

PP application note 32: The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [PP0056] for details).

6.1.4.3 FDP_UCT.1 Inter-TSF-Transfer

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

6.1.4.3.1 FDP_UCT.1 Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the ***PACE V2 Access Control SFP*** to be able to ***transmit and receive*** user data in a manner protected from unauthorised disclosure.

PP application note 33: FDP_UCT.1 and FDP_UIT.1 require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of PACE V2 Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

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

6.1.4.4 FDP_UIT.1 Data exchange integrity - MRTD

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the ***PACE V2 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, insertion and replay*** has occurred.

6.1.5 Class FMT Security Management

PP application note 34: 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).

6.1.5.1.1 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. Personalization,*** ***3. Configuration.***

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

6.1.5.1.2 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles ***1. Manufacturer,*** ***2. Personalization Agent,*** ***3. Supplemental Inspection System.***
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

PP application note 35: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

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

6.1.5.1.3 FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:

Deploying Test Features after TOE Delivery does not allow

1. ***User Data to be disclosed or manipulated***
2. ***TSF data to be disclosed or manipulated***
3. ***software to be reconstructed and***
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).

6.1.5.1.4 FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

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

Deploying Test Features after TOE Delivery does not allow

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

PP application note 36: The formulation of “Deploying Test Features …” in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy. Note that the term “software” in item 3 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

PP application note 37: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

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.

6.1.5.1.5 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

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to ***write*** the ***Initialization Data and Pre-personalization Data*** to ***the Manufacturer***.

PP application note 38: 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 Authentication Key.

6.1.5.1.6 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

FMT_SMR.1 Security roles

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to ***disable read access for users to*** the ***Initialization Data*** to ***the Personalization Agent***.

PP application note 39: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

6.1.5.1.7 FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to write the D***ocument PACE V2 Access Keys*** to ***the Personalization Agent***.

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to ***read*** the ***Document PACE V2 Access Keys and Personalization Agent Keys*** to ***none***.

PP application note 40: The Personalization Agent generates, stores and ensures the correctness of the Document PACE V2 Access Keys.

6.1.6 Class Protection of the Security Functions (FPT)

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.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 ar-

chitecture 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_EMSEC.1)" as specified below (Common Criteria Part 2 extended).

6.1.6.1.1 FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_EMSEC.1.1	The TOE shall not emit **variations in power consumption or timing during command execution**[33] in excess of **non-useful information**[34] enabling access to ***Personalization Agent Keys*** and **confidential user data**[35].
FPT_EMSEC.1.2	The TSF shall ensure ***any users*** are unable to use the following interface: **smart card circuit contacts or contactless interface**[36] to gain access ***to Personalization Agent Key(s)*** and **confidential user data**[37].

PP application note 41: <applied>

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).

6.1.6.1.2 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 out-of-range operating conditions where therefore a malfunction could occur,*** ***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).

6.1.6.1.3 FPT_TST.1 TSF testing

Hierarchical to:	No other components.
Dependencies:	No Dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests **during initial start-up**[38] to demonstrate the correct operation of ***the TSF***.

[33] [assignment: types of emissions]

[34] [assignment: specified limits]

[35] [assignment: list of types of user data]

[36] [assignment: type of connection]

[37] [assignment: list of types of 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.

PP application note 42: <applied>

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

6.1.6.1.4 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.

PP application note 43: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

PP application note 44: The SFRs "Non-bypassability of the TSF FPT_RVM.1" and "TSF domain separation FPT_SEP.1" are no longer part of [CC_2]. These requirements are now an implicit part of the assurance requirement ADV_ARC.1.

6.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following component:

ALC_DVS.2 and AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following Table 8 provides an overview for security functional requirements coverage.

[38] [*selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	X	X	X					
FCS_CKM.4	X		X					
FCS_COP.1/SHA	X	X	X					
FCS_COP.1/ENC	X	X	X					
FCS_COP.1/AUTH	X	X						
FCS_COP.1/MAC	X	X	X					
FCS_RND.1	X	X	X					
FIA_UID.1			X	X				
FIA_AFL.1			X	X				
FIA_UAU.1			X	X				
FIA_UAU.4	X	X	X					
FIA_UAU.5	X	X	X					
FIA_UAU.6	X	X	X					
FDP_ACC.1	X	X	X					
FDP_ACF.1	X	X	X					
FDP_UCT.1	X	X	X					
FDP_UIT.1	X	X	X					
FMT_SMF.1	X	X	X					
FMT_SMR.1	X	X	X					
FMT_LIM.1								X
FMT_LIM.2								X
FMT_MTD.1/INI_ENA				X				
FMT_MTD.1/INI_DIS				X				
FMT_MTD.1/KEY_WRITE	X	X	X					
FMT_MTD.1/KEY_READ	X	X	X					
FPT_EMSEC.1	X				X			
FPT_TST.1					X		X	
FPT_FLS.1	X				X		X	
FPT_PHP.3	X				X	X		

Table 8: Coverageo f Security Objective for the TOE by SFR

The security objective **OT.AC_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1 and FDP_ACF.1 as follows: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4 and FIA_UAU.5. The Personalization Agent can be authenticated either by using the PACE V2 mechanism (FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC) with the personalization key or for reasons of interoperability with the [PP0056] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the PACE V2 mechanism the SFR FIA_UAU.6 describes the re-authentication and FDP_UCT.1 and FDP_UIT.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC as well as FCS_COP.1/MAC for the ENC_MAC_Mode.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) setting the Document PACE V2 Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data. The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensure together with the SFR FCS_CKM.4, FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6 using either FCS_COP.1/ENC and FCS_COP.1/MAC or FCS_COP.1/AUTH.

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data by means of the PACE V2 mechanism. The SFR FIA_UAU.6, FDP_UCT.1 and FDP_UIT.1 requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1, FCS_COP.1/SHA, FCS_RND.1 (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document PACE V2 Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The read access to the logical MRTD data is defined by the FDP_ACC.1 and FDP_ACF.1.2: the successful authenticated Personalization Agent is allowed to read the data of the logical MRTD (EF.DG1 to EF.DG16). The successful authenticated Supplemental Inspection System is allowed to read the data of the logical MRTD (EF.DG1, EF.DG2 and EF.DG5 to EF.DG16). The SFR FMT_SMR.1 lists the roles (including Personalization Agent and Supplemental Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document PACE V2 Access Keys).

The SFR FIA_UAU.4 prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforces the TOE to accept the authentication attempt as Supplemental Inspection

System only by means of the PACE V2 Access Control Authentication Mechanism with the Document PACE V2 Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with PACE V2 Access Control Authentication Mechanism which includes the protection of the transmitted data in ENC_MAC_Mode by means of the cryptographic functions according to FCS_COP.1/ENC and FCS_COP.1/MAC (cf. the SFR FDP_UCT.1 and FDP_UIT.1). (for key generation), and FCS_COP.1/ENC and FCS_COP.1/MAC for the ENC_MAC_Mode. The SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA and FCS_RND.1 establish the key management for the secure messaging keys. The SFR FMT_MTD.1/KEY_WRITE addresses the key management and FMT_MTD.1/KEY_READ prevents reading of the Document PACE V2 Access Keys.

Note, neither the security objective **OT.Data_Conf** nor the SFR FIA_UAU.5 requires the Personalization Agent to use the PACE V2 Access Control Authentication Mechanism or secure messaging.

The security objective **OT.Identification** “Identification and Authentication of the TOE” addresses the storage of the IC Identification Data uniquely identifying the MRTD’s chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU_SAS.1.

Furthermore, the TOE shall identify itself only to a successful authenticated Supplemental Inspection System in Phase 4 “Operational Use”. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective OT.Identification. The SFR FIA_UID.1 and FIA_UAU.1 do not allow reading of any data uniquely identifying the MRTD’s chip before successful authentication of the Supplemental Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1 enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

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 MRTD’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_EMSEC.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.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.

6.3.2 Dependency Rationale

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

The following Table 9 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAS.1	No dependencies	n.a.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction,	Fulfilled by FCS_COP.1/ENC and FCS_COP.1/MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by FCS_CKM.1/3DES and FCS_CKM.1/AES
FCS_COP.1/SHA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/3DES AND FCS_CKM.1/AES Fulfilled by FCS_CKM.4
FCS_COP.1/ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/3DES AND FCS_CKM.1/AES, Fulfilled by FCS_CKM.4
FCS_COP.1/AUTH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 1 for non-satisfied dependencies justification 1 for non-satisfied dependencies
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/3DES AND FCS_CKM.1/AES, Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_UID.1	No dependencies	n.a.
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.4	No dependencies	n.a.
FIA_UAU.5	No dependencies	n.a.

SFR	Dependencies	Support of the Dependencies
FIA_UAU.6	No dependencies	n.a.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1, justification 2 for non-satisfied dependencies
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FDP_IFC.1 Subset information flow control or FDP_ACC.1 Subset access control]	justification 3 for non-satisfied dependencies Fulfilled by FDP_ACC.1
FMT_SMF.1	No dependencies	n.a.
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FMT_MTD.1/KEY_WRITE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1
FPT_EMSEC.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.

Table 9: Dependencies between the SFR for the TOE

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

No. 1: The SFR FCS_COP.1/AUTH uses the symmetric Personalization Key permanently stored during the Pre-Personalization process (cf. FMT_MTD.1/INI_ENA) by the manufacturer. Thus there is neither the necessity to generate or import a key during the addressed TOE lifecycle by the means of FCS_CKM.1/3DES

AND FCS_CKM.1/AES or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

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

No. 3: The SFR FDP_UCT.1 and FDP_UIT.1 require the use secure messaging between the MRTD and the BIS. There is no need for SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

6.3.3 Security Assurance Requirements Rationale

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

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the 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.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

The component AVA_VAN.5 augmented to EAL4 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

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

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

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

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security

Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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

7 TOE Summary Specification

7.1 Security Functionality

7.1.1 TSF_Access: Access rights

This security functionality manages the access to objects (files, directories, data and secrets) stored in the applet's file system. It also controls write access of initialization, pre-personalization and personalization data. Access control for initialization and pre-personalization in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP Java Card platform (SF.AccessControl, SF.I&A).

Access is granted (or denied) in accordance to access rights that depend on appropriate identification and authentication mechanisms.

TSF_Access covers the following SFRs:

- FIA_UID.1 requires that the TSF shall allow reading specific data on behalf of the user to be performed before the user is identified, but shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.1 requires that the TSF shall allow reading of specific data on behalf of the user to be performed before the user is authenticated, but shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.4 requires that the TSF shall prevent reuse of authentication data. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a (1) Basic Access Control Authentication Mechanism and a (2) Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user's claimed identity according to specified rules. TSF_Access realizes the appropriate control of the access rights.
- FIA_UAU.6 requires that the TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism. TSF_Access realizes the appropriate control of the access rights.
- FIA_AFL.1 requires that the TSF shall detect when a defined number of unsuccessful authentication attempts related to BAC authentication has occurred, and that if this number has been met, the TSF shall block the card permanently. This is realized by TSF_Auth_PACE-V2 and TSF_Access.
- FDP_ACC.1.1 requires that the TSF shall enforce the Basic 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. TSF_Access realizes the appropriate control of the access rights.
- FDP_ACF.1.1 requires that the TSF shall enforce the Basic Access Control SFP to objects based on the following: (1) Subjects: (a) Personalization Agent, (b) Basic Inspection System, (c) Terminal; (2) Objects: (a) data EF.DG1 to EF.DG16 of the logical MRTD, (b) data in EF.COM, (c) data in EF.SOD; (3) Security attributes: (a) authentication status of terminals. FDP_ACF.1.2 requires that the TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD, and (2) the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD. FDP_ACF.1.3 requires that

the TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none. This means that no other access possibilities exist. FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on the rule: (1) any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD; (2) any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD; (3) the Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4. TSF_Access realizes the appropriate control of the access rights.

- FDP_UCT.1: FDP_UCT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure. TSF_Access realizes the appropriate control of the access rights.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors. TSF_Access realizes the appropriate control of the access rights.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1) manufacturer, (2) personalization agent, and (3) basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.1: FMT_LIM.1.1 requires that the TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow (1) User Data to be disclosed or manipulated, (2) TSF data to be disclosed or manipulated, (3) software to be reconstructed and (4) substantial information about construction of TSF to be gathered which may enable other attacks. TSF_Access realizes the appropriate control of the access rights.
- FMT_LIM.2: FMT_LIM.2.1 requires that 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 disclosed or manipulated, (2) TSF data to be disclosed or manipulated, (3) software to be reconstructed and (4) substantial information about construction of TSF to be gathered which may enable other attacks. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document PACE V2 Access Keys to the Personalization Agent. This is realized by TSF_Admin, TSF_Access and TSF_OS. TSF_Access realizes the appropriate control of the access rights.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document PACE V2 Access Keys and Personalization Agent Keys to none. This is realized by TSF_Admin, TSF_Secret, TSF_Access and TSF_OS. TSF_Access realizes the appropriate control of the access rights.

7.1.2 TSF_Admin: Administration

This Security Functionality manages the storage of manufacturing data, pre-personalization data and personalization data. This storage area is a write-only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Management of manufacturing and pre-personalization data in Phase 2 – while the actual applet is not yet present – is based on the card manager of the underlying JCOP Java Card platform (SF.SecureManagement); also Audit functionality is based on JCOP functionality (SF.Audit). During Operational Use phase, read access is only possible after successful authentication.

TSF_Admin covers the following SFRs:

- FAU_SAS.1: FAU_SAS.1 requires that the TSF shall provide the Manufacturer with the capability to store the IC Identification Data in the audit records. This is realized by TSF.Admin.

- FMT_SMF.1: FMT_SMF.1.1 requires that the TSF shall be capable of performing the following management functions: (1) initialization, (2) pre-personalization, and (3) personalization. This is realized by TSF_Admin.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles (1) manufacturer, (2) personalization agent, and (3) basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. TSF_Admin provides the according storage area for manufacturing data, pre-personalization data and personalization data.

7.1.3 TSF_Secret: Secret key management

This Security Functionality ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These functions make use of SF.CryptoKey of the underlying JCOP Java Card OS.

TSF_Secret covers the following SFRs:

- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document PACE V2 Access Keys to the Personalization Agent. This is realized by TSF_Secret, TSF_Access and TSF_OS.
- FMT_MTD.1/KEY_READ: FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none. This is realized by TSF_Secret, TSF_Access and TSF_OS.

7.1.4 TSF_Crypto: Cryptographic operations

This Security Functionality performs high level cryptographic operations. The implementation is based on the Security Functionalities provided by TSF_OS.

TSF_Crypto covers the following SFRs:

- FCS_CKM.1.1 requires that the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (Document PACE V2 Access Key Derivation Algorithm) and specified cryptographic key sizes of 112 or 128, 192 and 256 bit. This is realized within TSF_Crypto and TSF_OS.
- FCS_CKM.4: FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physically overwriting the keys with zeros by method (e.g. clearKey of [Java_RES]) or automatically on applet deselection. This is mainly realized by TSF_OS; for the CMAC Sub-Keys (for Secure Messaging) TSF_Crypto is also used.
- FCS_COP.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with Triple-DES or AES Retail-MAC and cryptographic key sizes of 112 or 128, 192, 256 bit that meet ISO 9797-1 [ISO9797-1] or SP 800-38b [SP800-38b]. The algorithm is realized by TSF_Crypto, while TSF_OS provides the basic Triple-DES implementation and TSF_SecureMessaging provides the secure messaging protocol.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a Basic Access Control Authentication Mechanism and a Symmetric Authentication Mechanism based on Triple-DES to support user authentication. The according cryptographic functions are realized by TSF_Crypto (based on functions provided by TSF_OS).

7.1.5 TSF_ SecureMessaging: Secure Messaging

This Security Functionality realizes a secure communication channel after successful authentication for personalization and BAC during operational use.

TSF_SecureMessaging covers the following SFRs:

- FCS_COP.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with Triple-DES or AES Retail-MAC and cryptographic key sizes of 112 or 128, 192, 256 bit that meet ISO 9797-1 [ISO9797-1] or SP 800-38b [SP800-38b]. The implementation is realized by TSF_SecureMessaging.
- FDP_UIT.1: FDP_UIT.1.2 requires that the TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred. This is realized by TSF_SecureMessaging.

7.1.6 TSF_Auth_PACE-V2: PACE Authentication protocol

This security function realizes the PACE authentication mechanism. TSF_Auth_PACE-V2 covers the following SFRs:

- FIA_UID.1: FIA_UID.1.1 requires that the TSF shall allow to read the Initialization Data in Phase 2 “Manufacturing”, to read the random identifier in Phase 3 “Personalization of the MRTD”, and to read the random identifier in Phase 4 “Operational Use” on behalf of the user to be performed before the user is identified. The authentication mechanism leads to the identification and is provided by TSF_Auth_PACE-V2.
- FIA_UAU.1: FIA_UAU.1.1 requires that the TSF shall allow reading the Initialization Data in Phase 2 “Manufacturing”, to read the random identifier in Phase 3 “Personalization of the MRTD”, and to read the random identifier in Phase 4 “Operational Use” on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 requires that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. The authentication mechanism is provided by TSF_Auth_PACE-V2.
- FIA_UAU.4: FIA_UAU.4.1 requires that the TSF shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism, and Authentication Mechanism based on Triple-DES. The authentication mechanisms are provided by TSF_Auth_PACE-V2.
- FIA_UAU.5: FIA_UAU.5.1 requires that the TSF shall provide a Basic Access Control Authentication Mechanism and a Symmetric Authentication Mechanism based on Triple-DES to support user authentication. FIA_UAU.5.2 requires that the TSF shall authenticate any user’s claimed identity according to specified rules. The authentication mechanisms are provided by TSF_Auth_PACE-V2.
- FIA_UAU.6: FIA_UAU.6.1 requires that the TSF shall re-authenticate the user under the conditions each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism. The authentication mechanism is provided by TSF_Auth_PACE-V2.
- FIA_AFL.1: FIA_AFL.1.1 requires that the TSF shall detect when an administrator configurable positive integer within 1 – 32767 unsuccessful authentication attempts occur related to BAC authentication. FIA_AFL.1.2 requires that when the defined number of unsuccessful authentication attempts has been met, the TSF shall block the card permanently. The authentication mechanism is provided by TSF_Auth_PACE-V2.
- FDP_ACC.1: FDP_ACC.1.1 requires that the TSF shall enforce the Basic 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 authentication mechanism is provided by TSF_Auth_PACE-V2.
- FDP_ACF.1: FDP_ACF.1.1 requires that the TSF shall enforce the Basic Access Control SFP to objects based on defined subjects, objects, security attributes. FDP_ACF.1.2 requires that the TSF shall enforce the defined rules to determine if an operation among controlled subjects and controlled objects is allowed. FDP_ACF.1.3 requires that no other access possibilities exist. FDP_ACF.1.4 requires that the TSF shall explicitly deny access of subjects to objects based on defined rules. The authentication mechanism for the Basic Access Control SFP is provided by TSF_Auth_PACE-V2.

- FDP_UCT.1: FDP_UCT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure. The authentication mechanism for the Basic Access Control SFP is provided by TSF_Auth_PACE-V2.
- FDP_UIT.1: FDP_UIT.1.1 requires that the TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors. The authentication mechanism for the Basic Access Control SFP is provided by TSF_Auth_PACE-V2.
- FMT_SMR.1: FMT_SMR.1.1 requires that the TSF shall maintain the roles manufacturer, personalization agent, and basic inspection system. FMT_SMR.1.2 requires that the TSF shall be able to associate users with roles. The according authentication mechanism is provided by TSF_Auth_PACE-V2.
- FMT_LIM.1: FMT_LIM.1.1 requires that the TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The according authentication mechanism is provided by TSF_Auth_PACE-V2.
- FMT_LIM.2: FMT_LIM.2.1 requires that 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 User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and substantial information about construction of TSF to be gathered which may enable other attacks. The according authentication mechanism is provided by TSF_Auth_PACE-V2.

7.1.7 TSF_Integrity: Integrity protection

This Security Functionality protects the integrity of internal applet data like the Access control lists. This function makes use of SF.SecureManagement and SF.Transaction of the underlying JCOP Java Card OS (cf. the according security target [ST_JCOP081]).

TSF_Integrity covers the following SFRs:

- FPT_FLS.1: FPT_FLS.1.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) exposure to out-of-range operating conditions where therefore a malfunction could occur, and (2) failure detected by TSF according to FPT_TST.1. This is realized by TSF_Integrity and TSF_OS.

7.1.8 TSF_OS: Javacard OS security functions

The Javacard operation system (part of the TOE) features the following Security Functionalities. The exact description can be found in the Javacard OS security target [ST_JCOP081]; the realization is partly based on the security functions of the certified cryptographic library and the certified IC platform:

- Enforcement of access control (SF.AccessControl)
- Audit functionality (SF.Audit)
- Cryptographic key management (SF.CryptoKey)
- Cryptographic operations (SF.CryptoOperation)
- Identification and authentication (SF.I&A)
- Secure management of TOE resources (SF.SecureManagement)
- Transaction management (SF.Transaction)

Since the applet layer of the TOE is based on the Javacard OS, the realization of all TOE security functionalities and thus the fulfillment of all SFRs has dependencies to TSF_OS. The following items list all SFRs where TSF_OS has an impact above this level:

- FCS_CKM.1: FCS_CKM.1.1 requires that the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm (Document Basic Access Key Derivation Algorithm) and specified cryptographic key sizes of 112 or 128, 192 and 256 bit bit. This is realized by TSF_OS.
- FCS_CKM.4.1 requires that the TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method. This is realized in the security functions provided by TSF_OS. The only exceptions are the CMAC Sub-Keys (for Secure Messaging), where the security functionality is provided by TSF_Crypto.
- FCS_COP.1.1/SHA: FCS_COP.1.1/SHA requires that the TSF shall perform hashing in accordance with a specified cryptographic algorithm (SHA-1, SHA-224 or SHA-256) that meets: FIPS 180-4. This is realized by TSF_OS.
- FCS_COP.1.1/ENC : FCS_COP.1.1/ENC requires that the TSF shall perform secure messaging (BAC) – encryption and decryption in accordance with a specified cryptographic algorithm (Triple-DES in CBC mode) and cryptographic key sizes of 112 bit that meet FIPS 46-3. This is realized by TSF_OS.
- FCS_COP.1.1/AUTH: FCS_COP.1.1/AUTH requires that the TSF shall perform symmetric authentication (encryption and decryption) in accordance with a specified cryptographic algorithm (Triple-DES) and cryptographic key sizes of 112 bit that meet FIPS 46-3. This is realized by TSF_OS.
- FCS_COP.1.1/MAC: FCS_COP.1.1/MAC requires that the TSF shall perform secure messaging with a message authentication code in accordance with a specified cryptographic algorithm (Retail MAC) and a cryptographic key size of 112 bit that meets ISO 9797. TSF_OS provides the basic cryptographic mechanisms.
- FCS_RND.1.1: FCS_RND.1.1 requires that the TSF shall provide a mechanism to generate random numbers that meet the AIS 20 Class K3 quality metric. This is realized by TSF_OS.
- FMT_MTD.1.1/INI_ENA requires that the TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer. The basic mechanisms are provided by TSF_OS.
- FMT_MTD.1.1/INI_DIS requires that the TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent. The basic mechanisms for this are provided by TSF_OS.
- FMT_MTD.1.1/KEY_WRITE requires that the TSF shall restrict the ability to write the Document Basic Access Keys to the Personalization Agent. The basic mechanisms are provided by TSF_OS.
- FMT_MTD.1.1/KEY_READ requires that the TSF shall restrict the ability to read the Document Basic Access Keys and Personalization Agent Keys to none. The basic mechanisms are provided by TSF_OS.
- FPT_EMSEC.1.1 requires that the TOE shall not emit variations in power consumption or timing during command execution in excess of non-useful information enabling access to Personalization Agent Key(s) and confidential user data. FPT_EMSEC.1.2 requires that the TSF shall ensure any unauthorized users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and confidential user data. This is mainly realized by appropriate measures in TSF_OS together with the strict following of the security implementation guidelines of the Javacard platform.
- FPT_FLS.1.1 requires that the TSF shall preserve a secure state when the following types of failures occur: (1) exposure to out-of-range operating conditions where therefore a malfunction

could occur, and (2) failure detected by TSF according to FPT_TST.1. This is realized by TSF_OS (together with and TSF_Integrity).

- FPT_TST.1.1 requires that the TSF shall run a suite of self tests during initial start-up to demonstrate the correct operation of the TSF. FPT_TST.1.2 requires that the TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.3 requires that the TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.
- FPT_PHP.3.1 requires that the TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced. This all is realized by TSF_OS, in parts due to the characteristics of the hardware platform.

7.2 Mapping of TOE Security Requirements and TOE security functionalities

Each TOE security functional requirement is implemented by at least one security function. The mapping of TOE Security Requirements and TOE security functionalities is given in the following table. If iterations of a TOE security requirement are covered by the same TOE security functionality the mapping will appear only once. The description of the TSF is given in section 7.1.

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth_PACE-V2	TSF_Integrity	TSF_OS
FAU_SAS.1		x						
FCS_CKM.1				X				x
FCS_CKM.4				X				x
FCS_COP.1/SHA								x
FCS_COP.1/ENC								x
FCS_COP.1/AUTH								x
FCS_COP.1/MAC				x	x			x
FCS_RND.1								x
FIA_UID.1	x					x		
FIA_UAU.1	x					x		
FIA_UAU.4	x					x		
FIA_UAU.5	x			x		x		
FIA_UAU.6	x					x		
FIA_AFL.1	x					x		
FDP_ACC.1	x					x		
FDP_ACF.1	x					x		
FDP_UCT.1	x					x		

	TSF_Access	TSF_Admin	TSF_Secret	TSF_Crypto	TSF_SecureMessaging	TSF_Auth_PACE-V2	TSF_Integrity	TSF_OS
FDP_UIT.1	x				x	x		
FMT_SMF.1		x						
FMT_SMR.1	x	x				x		
FMT_LIM.1	x					x		
FMT_LIM.2	x					x		
FMT_MTD.1/INI_ENA								x
FMT_MTD.1/INI_DIS								x
FMT_MTD.1/KEY_WRITE	x		x					x
FMT_MTD.1/KEY_READ	x		x					x
FPT_EMSEC.1								x
FPT_FLS.1							x	x
FPT_TST.1								x
FPT_PHP.3								x

Table 10: Mapping of TOE Security Requirements and TOE security functionalities.

References

In the following tables, the references used in this document are summarized. The first column lists the internal reference names, the third (last) column – if applicable – the reference numbers in to these documents or older versions of these documents in the protection profile "Machine Readable Travel Document - SAC/PACE V2 Access Control" [PP_SAC].

Common Criteria

[CC_1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009	[1]
[CC_2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009	[2]
[CC_3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009	[3]
[CC_4]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009	[4]
[AIS_32]	Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema; Bundesamt für Sicherheit in der Informationstechnik Version 1, 02.07.2001	[5]

Protection Profiles

[PP0002]	PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001	[16]
[PP0035]	Security IC Platform Protection Profile, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007	[17]
[PP0056]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0056, version 1.10, 25th March 2009	[18]
[PP_SAC]	Common Criteria Protection Profile — Machine Readable Travel Document - SAC/PACE V2 Access Control, Agence Nationale des titres sécurisés – ANTS, Version 1.0, 21th September 2010	-
[PP_Javacard]	Java Card System - Minimal Configuration Protection Profile, Version 1.1, May 2006, part of: Java Card Protection Profile Collection, Version 1.1, May 2006	-

TOE and Platform References

[Guidance]	cv act ePasslet/EACv2-SAC – cv act ePasslet Suite Java Card applets providing	-

	ePass/eID application with Supplemental Access Control (SAC) and Extended Access Control version 2 (EACv2), Guidance Manual, Version 1.3.1; cryptovision, June 2012	
[ZertIC040]	Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification; BSI, July 2007.	-
[ZertIC080]	Certification Report BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B, each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH; BSI, July 2007.	-
[ZertIC081]	Certification Report BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A, each with IC dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification; BSI, November 2009.	-
[ZertJCOP040]	Certification Report BSI-DSZ-CC-0730-2011 for NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, May 2011.	-
[ZertJCOP080],	Certification Report BSI-DSZ-CC-0674-2011 for NXP J3A080 and J2A080 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, March 2011.	-
[ZertJCOP081]	Certification Report BSI-DSZ-CC-0675-2011 for NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH; BSI, April 2011.	-
[ZertCL040]	Certification Report BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B /P5CC040V0B / P5CD020V0B / P5CC021V0B /P5CD012V0B from NXP Semiconductors Germany GmbH; BSI, January 2011.	-
[ZertCL080]	Certification Report BSI-DSZ-CC-0709-2010 for Crypto Library V2.6 on P5CD080V0B /P5CN080V0B / P5CC080V0B / P5CC073V0B from NXP Semiconductors Germany GmbH; BSI, December 2010.	-
[ZertCL081]	Certification Report BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A /P5CC081V1A / P5CN081V1A / P5CD041V1A /P5CD021V1A / P5CD016V1A from NXP Semiconductors Germany GmbH; BSI, November 2010.	-
[ST_JCOP040]	Security Target Lite „NXP J3A040 and J2A040 Secure Smart Card Controller Rev. 3“, Rev. 01.03; NXP, 13 May 2011.	-
[ST_JCOP080]	Security Target Lite „NXP J3A080 and J2A080 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010.	-
[ST_JCOP081]	Security Target Lite „NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Rev. 3“, Rev. 01.02; NXP, December 2010.	-
[ST_CL040]	Security Target Lite “Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B”, Rev. 2.4; NXP, 14 December 2010.	-
[ST_CL080]	Security Target Lite “Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B”, NXP, Rev. 2.3; NXP, 12 November 2010.	-

[ST_CL081]	Security Target Lite "Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A", NXP, Rev. 1.2; 9 November 2010.	-
[ST_IC040]	Security Target Lite "P5CD040/P5CC040/P5CD020/P5CC021 V0B", Rev. 1.0, NXP, 21 March 2007.	-
[ST_IC080]	Security Target Lite "P5CD080/P5CN080/P5CC080 V0B", Rev. 1.0, NXP, 21 March 2007.	-
[ST_IC081]	Security Target Lite "NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A", Rev. 1.3, NXP, 21 September 2009.	-
[JCOP_UGM]	NXP JCOP V2.4.1 Revision 3 secure smart card controller, Rev. 3.0--9 March 2011 – User manual, Doc No. 188830	-

ICAO specifications

[ICAODoc]	ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization	[6]
[ICAOFal]	INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)	[7]
[ICAOTR]	ICAO TR – Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2011	[20]

Cryptography

[FIPS46-3]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology	[9]
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, March 2012	
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001	[12]
[ISO9797-1]	ISO 9797-1:1999 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher	
[SP800-38b]	NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Auhentication, May 2005	

Other References

[ISO7816-4]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004	[21]
[TR03110]	Technical Guideline Advanced Security Mechanisms for Machine Readable	[19]

	Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)	
[Java_RES]	Runtime Environment Specification, Java Card(tm) Platform, Version 2.2.2, March 2006, Sun Microsystems	[23]

Glossary

Active authentication	Security mechanism defined in [MRTD-PKI] 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.
AES	The AES (Advanced Encryption Standard) has been defined as a standard for symmetric data encryption. It is a block cipher with a block length of 128 bit and key lengths of 128, 192 and 256 bit.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Asymmetric cipher	Encryption procedures employing two different keys (in contrast to a symmetric cipher): one publicly known (public key) for data encryption and one key only known to the message receiver (private key) for decryption.
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authentication	Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.
BAC	Basic access control. Security mechanism defined in [MRTD-PKI] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging.
Basic access keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [MRTD-PKI]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys, derived from the printed MRZ data, for reading the logical MRTD.
Biographical data (biodata)	The personalized details of the MRTD holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [ICAODoc]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Block cipher	An algorithm processing the plaintext in bit groups (blocks). Its alternative is called stream cipher.
CA	Certification authority
Card Access Number (CAN)	Password derived from a short number printed on the front side of the datapage. [ICAOTR]
Certificate	See digital certificate
Certificate revocation list	A list of revoked certificates issued by a certificate authority
Certification authority	An entity responsible for registering and issuing, revoking and generally managing digital certificates

Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAODoc]
Country signing CA certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (KPuCSCA) issued by Country Signing Certification Authority. The C_{CSCA} is stored in the inspection system.
Country verifying CA	The country specific root of the PKI of Inspection Systems. It creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing country or organization in respect to the protection of sensitive biometric data stored in the MRTD.
CRL	see Certificate Revocation List
Cryptography	In the classical sense, the science of encrypting messages. Today, this notion comprises a larger field and also includes problems like authentication or digital signatures.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CVCA link certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
DES	(Data Encryption Standard) symmetric 64 bit block cipher, which was developed (first under the name Lucifer) by IBM. The key length is 64 bit of which 8 bit serve for a parity check. DES is the classic among the encryption algorithms, which nevertheless is no longer secure due to its insufficient key length. Alternatives are Triple-DES or the successor AES.
Digital certificate	A data set that identifies the certification authority issuing it, identifies its owner, contains the ower's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.
Digital signature	The counterpart of a handwritten signature for documents in digital format. A digital signature grants authentication, integrity, and non-repudiation. These features are achieved by using asymmetric procedures.
Document PACE V2 Access Keys	Pair of symmetric keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAOTR]. It is drawn from the printed MRZ or CAN of the passport book to authenticate an entity able to read these data.
Document verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
EAC	Extended access control. Security mechanism identified in [MRTD-PKI] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Eavesdropper	A threat agent with high attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
ECC	(Elliptic Curve Cryptography) class of procedures providing an attractive alterna-

	tive for the probably most popular asymmetric procedure, the RSA algorithm.
Elliptic curves	A mathematical construction, in which a part of the usual operations applies, and which has been employed successfully in cryptography since 1985.
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. [ICAODoc]
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Supplemental Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAODoc]
Hash function	A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value. Common hash functions are RIPEMD-160 and SHA-1, each having hash values with a length of 160 bit as well as the MD5, which is still often used today having a hash value length of 128 bit.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
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. [ICAODoc]
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. [ICAODoc]
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD’s material (IC identification data).
Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD’s chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAODoc]
Issuing State	The Country issuing the MRTD. [ICAODoc]
Javacard	A smart card with a Javacard operation system.

Key exchange	The use of symmetric cipher procedures requires that two communication partners decide on one joint key only known to themselves. The difficulty is that for the exchange of such information usually only partially secure channels exist. Additionally, protocols for key exchange must be prepared in such a way that only those pieces of information are exchanged which do not lead to knowledge of the real secret (the key). The most popular protocol of that type is diffie-Hellman, whose presentation in 1976 can be regarded as the birth of public key cryptography.
LDS	Logical data structure. The collection of groupings of data elements stored in the optional capacity expansion technology, defined in [MRTD-LDS].
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAODoc] as specified by ICAO on the integrated circuit. It presents readable data including (but not limited to) 1. personal data of the MRTD holder 2. the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3. the digitized portraits (EF.DG2), 4. the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5. the other data according to LDS (EF.DG5 to EF.DG16). 6. EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the integrated circuit including (but not limited to) 1. data contained in the machine-readable zone (mandatory), 2. digitized photographic image (mandatory) and 3. fingerprint image(s) and/or iris image(s) (optional).
MAC	Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy, requires its protection in a suitable way.
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAODoc]
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. [ICAODoc]
MRTD	Machnine-readable travel document. Official document issued by a State or Organization 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.
MRTD PACE V2 Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

MRZ	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. It also means the password derived from the MRZ. [ICAODoc]
Non-repudiation	One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered and respective framework conditions need to be provided by pertinent laws.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
PACE V2/Supplemental Access Control (SAC)	Security mechanism defined in [ICAOTR] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document PACE V2 Access Keys (see there).
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Passphrase	A long, but memorable character sequence (e.g. short sentences with punctuation) which should replace passwords as they offer more security.
Password	A secret character sequence whose knowledge is to serve as a replacement for the authentication of a participant. A password is usually short to really ensure that an attacker cannot guess the password by trial and error.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment". [ICAODoc]
Personalization agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. other data.

PKI	Cf. Public Key Infrastructure
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.
Pre-personalized MRTD's chip	MRTD's chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	An inspection system that contains a terminal for the communication with the MRTD's chip and does not implement the terminals part of the PACE V2 Access Control Mechanism. This PP does not support PIS
Private key	Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.
Pseudo random number	Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo-random number generators are used, which then should be initialized with a real random element (the so called *seed*).
Public key	Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.
Public key infrastructure (PKI)	Combination of hardware and software components, policies, and different procedures used to manage digital certificates.
Random numbers	Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for a software), so called pseudo random numbers are used instead.
Receiving State	The Country to which the Traveler is applying for entry. [ICAODoc]
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.
SAC	Cf. PACE V2/Supplemental Access Control (SAC).
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [ICAODoc]
Secure messaging	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
SFR	Security functional requirement.
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Smart card	A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (ROM, EEPROM) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all of their functionality comprised on a single chip (in

	contrast to chip cards, which contain several chips wired to each other). Therefore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.
SOD	Document Security Object (stored in EF.SOD). A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS).
Stream cipher	Symmetric encryption algorithm which processes the plaintext bit-by-bit or byte-by-byte. The other usually employed class of procedures comprises so called block cipher.
Supplemental Inspection System (SIS)	An inspection system which implements the terminals part of the PACE V2 Access Control Mechanism and authenticates itself to the MRTD's chip using the Document PACE V2 Access Keys, derived from the printed MRZ data or the CAN, for reading the logical MRTD.
Symmetric cipher	Encryption procedure using the same key for enciphering and deciphering (or, in which these two keys can simply be derived from each other). One distinguishes between block ciphers processing plaintext in blocks of fixed length (mostly 64 or 128 bit) and stream ciphers working on the basis of single characters.
TOE	Target of evaluation.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.
TSF	TOE security functionality.
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [CC_1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template.
Verification data	Data provided by an entity in an authentication attempt to prove their identityto the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
X.509	Standard for certificates, CRLs and authentication services. It is part of the X.500 standard of the ITU-T for realization of a worldwide distributed directory service realized with open system.

Acronyms

Acronym	Term
BIS	Basic Inspection System
CC	Common Criteria
EF	Elementary File

GIS	General Inspection System
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
n.a.	Not applicable
OSP	Organizational security policy
PT	Personalization Terminal
SAR	Security assurance requirements
SFR	Security functional requirement
SIS	Supplemental Inspection System
TOE	Target of Evaluation
TSF	TOE security functionality