Sealys eTravel SCOSTA-CL on G265-V3c Security Target Lite

UPDATES

Rev.	Date	Author	Modification
1.0	25-Aug-15	Gemalto	ST Lite initial version
1.1	02-Sep-15	Gemalto	ST Lite version updated according to the evaluated ST v1.6
1.1	23-Oct-15	Gemalto	ST Lite version updated according to the evaluated ST v1.7
1.3	30-Oct-15	Gemalto	ST Lite updated according to the evaluated ST v1.8 and CESG comments.

Table of contents

Table of figures

Table of tables

1 ST introduction

1.1 ST Identification

Title:	Gemalto Sealys eTravel SCOSTA-CL on G265-V3c Security Target Lite
Version:	1.3 issued on 30 October 2015
ST reference:	D1375202
Origin:	Gemalto
Product identification:	ScostaCL V3c
Security Controllers:	M7820 A11 SLE78CLX802P
TOE internal name[1]:	ScostaCL V3c BAC
TOE commercial name:	Gemalto Sealys eTravel SCOSTA-CL on G265-V3c
TOE documentation:	Operational User Guidance [OPE_MRTD] Preparative procedures [PRE_MRTD]
IT Security Evaluation scheme	UL
IT Security Certification scheme	National Technical Authority for Information Assurance (CESG)

The TOE identification is provided by the Card Production Life Cycle Data (CPLC) of the TOE, located in ROM. These data are available by executing a dedicated command (GET DATA with DO tag 0xDF7E).

[1] This internal name is used in the TOE development and security documentation.

CPLC field	Length	Value
Card Manufacturer	2	0x40 0x90
IC Type	2	0x71 0x72
Operating System Identifier	2	0x12 0x91
Operating System Version	2	0x01 0x00
Operating System Date	2	0xC2 0x30
Operating System Type	1	0xAA
IC Serial Number Byte 1-2: Chip type Byte 3: Batch Number Byte 4-5: Batch Number Byte 6: Wafer Number Byte 7: Die position Byte 8: Die position	8 2 1 2 1 1 1	Unique identification written by the IC Manufacturer Sales/development code – Chip Identification Number FAB number + year Business week + lot number Wafer of corresponding batch X-position of die on wafer Y-position of die on wafer

Table 1 TOE Identification Data

1.2 ST overview

The ST is based on Protection Profile *Machine Readable Travel Document with "ICAO Application", Basic Access Control* [PP-MRTD-BAC].

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) based on the requirements of the International Civil Aviation Organization (ICAO). More specifically the TOE consists of operating system of MRTD's chip with ICAO application. The TOE is programmed according to Logical Data Structure as defined in [ICAO-9303].

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

The main objectives of this ST are:

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

1.3 References

1.3.1 External References

[AIS20]	BSI, Application Notes and Interpretation of the Scheme (AIS) 20 – Functionality classes and evaluation methodology for deterministic random number generators, Version 2 (02.12.1999), English translation.
[BIO]	BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, version 3.1 rev 4, September 2012
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2012-09-002, version 3.1 rev 4, September 2012
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2012-09-003, version 3.1 rev 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2012-09-004, version 3.1 rev 4, September 2012
[CR-IC]	BSI, Certification Report, Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software , August 2015, BSI-DSZ-CC-0829-V2-2015
[FIPS180-4]	Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD (SHS), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, February 25, 2004
[FIPS46-3]	Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2005 May 19
[ICAO]	INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL) DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)
[ICAO-9303]	9303 Part 3 Vol 2 – ICAO Machine Readable Travel Document Third edition 2008
[ISO15946-1]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2008
[ISO15946-2]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures, 2002

[ISO15946-3]	ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment, 2002
[ISO7816]	ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, 2013
[ISO9796-2]	ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2010
[ISO9797-1]	ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 2011
[PKCS#3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, International Civil Aviation Organization Version 1.1, October 01 2004
[PP-IC-0035]	Smartcard IC Platform protection Profile, Version 1.0, 15 June 2007, BSI-PP-0035-2007
[PP-MRTD-BAC]	Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0055, version 1.10, 25th March 2009
[SOG-IS]	SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3.0, January 2010
[SS]	ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 2 Machine Readable Passports, Sixth Edition – 2006
[ST-IC]	Infineon Technologies AG , Security Target Lite, Smart card IC M7820 A11 RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software, version 1.9, July 2015

1.3.2 Internal References

[OPE_MRTD]	D1341110 Operational User Guidance – Sealys eTravel SCOSTA–CL on G265 - V3c
[PRE_MRTD]	D1341111 Preparative procedures – Sealys eTravel SCOSTA–CL on G265 - V3c

1.4 Acronyms and glossary

Acr.	Term	Definition
AA	Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
	Application note [PP-MRTD-EAC]	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 (cf. CC part 1, section B.2.7).
	Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
	Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system protects their communication by means of secure messaging with Basic Access Keys (see there).
BIS	Basic Inspection System	An inspection system which implements the terminal part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys drawn from printed MRZ data for reading the logical MRTD.
	Biographical data (biodata)	The personalized details of the bearer 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. [SS]
	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.
	Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [SS]
CPLCD	Card Production Life Cycle Data	The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command.
CSCA	Country Signing Certification Authority	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
CVCA	Country Verifying Certification Authority	The Country Verifying Certification Authority enforces the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems.

	Document Basic Access Keys	Pair of symmetric Triple-DES 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 [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.
DH	Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
DSO	Document Security Object	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). [PKI]
DV	Document Verifier	The Document Verifier enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The DV manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the Issuing State or Organization in form of the Document Verifier Certificates.
EAC	Extended Access Control	Security mechanism identified in [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 bysecure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
	Eavesdropper	A threat agent with moderate attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
EC-DH	Elliptic Curve Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
	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. [BIO]
EIS	Extended Inspection System	The EIS in addition to the General Inspection System (GIS) (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.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
GIS	General Inspection System	The GIS is a Basic Inspection System (BIS) which implements additionally the Chip Authentication Mechanism.

	Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [BIO]
	IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
	IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
	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. [SS]
	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. [BIO]
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
	Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [BIO]
IS	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). [ICAO-9303].
	Issuing State	The Country issuing the MRTD. [ICAO-9303]
LDS	Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.

	Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure (LDS) as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (2) the digitized portraits (EF.DG2), (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (4) the other data according to LDS (EF.DG5 to EF.DG16).
	Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless 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).
MRTD	Machine 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. [ICAO-9303]
MRV	Machine readable visa	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. [ICAO-9303]
MRZ	Machine Readable Zone	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. [ICAO-9303]
	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. [SS]
	MRTD administrator	The Issuing State or Organization which is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.
	MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: - the file structure implementing the LDS [ICAO-9303], - the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 and EF.DG16), - the TSF Data including the definition of the authentication data but without the authentication data itself.
	MRTD Basic 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.
	MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

	MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and ICAOT, [ICAO], p. 14. programmed according to the Logical Data Structure as specified by ICAOT, [ICAO], p. 14.
	MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
	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.
	Passive authentication	- verification of the digital signature of the Document Security Object - comparison the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	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 Key	Symmetric cryptographic authentication 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): - biographical data, - data of the machine-readable zone, - photographic image and - other data.
	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 Personalization Agent Key Pair.
	Pre –personalized MRTD's chip	MRTD's chip equipped with pre-personalization data.

PIS	Primary Inspection System	An inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
	Random identifier	Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability.
	Receiving State	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
	reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
	secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [SS]
	secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.
	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.
	TD1	Size 1 machine readable official travel document (TD-1): A card with nominal dimensions guided by those specified for the ID-1 type card (ISO/IEC 7810) (excluding thickness). In the case of a plastic card which carries any optional, additional data storage technology, the reading of which requires it to be inserted into a slot reader (i.e. magnetic stripe, optical memory or integrated circuit with contacts), the TD-1 conforms to the precise dimensions and tighter tolerances specified in ISO/IEC 7810.
	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. [BIO]
	traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
	TSF data	Data created by and for the TOE that might affect the operation of the TOE [CC-1].
	Unpersonalized MRTD	MRTD material prepared to produce a personalized MRTD containing an initialized and pre-personalized MRTD's chip.
	User data	Data created by and for the user, that does not affect the operation of the TSF [CC-1].
	Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [BIO]

	verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

1.5 TOE Overview

This Security Target defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [ICAO-9303].

1.5.1 TOE definition

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

1.5.2 TOE usage and security features for operational use

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 security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the 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) 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 trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

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

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

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

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

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

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

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This security target does not address the Active Authentication and the Extended Access control as optional security mechanisms.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic 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 [ICAO-9303], normative appendix 5.

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

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

1.6 TOE boundaries

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

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

- the Basic Access Control (BAC) according to the ICAO document [PKI]

The TOE comprises of:

- the circuitry of the MRTD's chip (the integrated circuit, IC),

- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application, and
- the associated guidance documentation.

Application note: Components within the TOE boundary are refined in the following manner:

- *the Integrated Circuit (IC),*
- *the IC Dedicated Test Software,*
- *the IC Dedicated Support Software,*
- *the ScostaCL V3c Embedded Software (ES) that includes (as shown in* Figure 1: TOE **Boundaries***)*
  - *the OS layers: HW Drivers and JKernel*
  - *the Scosta application*
- *part of the MRTD Logical Data Structure created before the personalization,*
- *the guidance documentation of the product:*
  - *the preparation guide (assurance family AGD-PRE* [PRE_MRTD]*),*
  - *the operational guide (assurance family AGD-OPE)* [OPE_MRTD]*.*

The ScostaCL Embedded Software (ES) is implemented in the ROM of the chip. The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent or from the Personalization Agent to the MRTD Manufacturer.

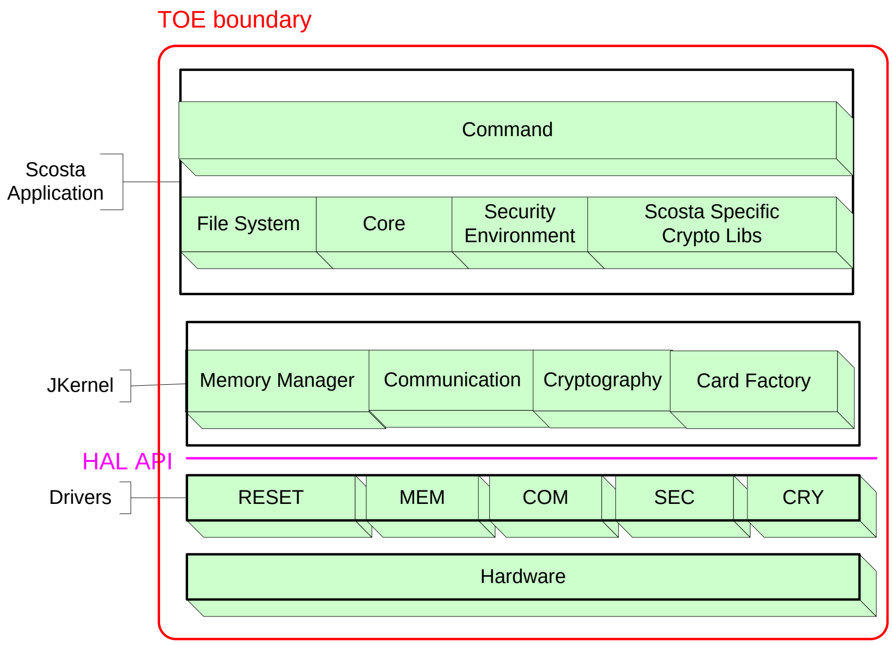

Figure 1: TOE Boundaries

1.7 Interfaces of the TOE

The software interfaces of the TOE consist of the specific APDU commands of the Scosta application.
The hardware interfaces of the TOE are already described in the security target of the IC [ST-IC].

1.8 TOE intended usage

State or organization issues MRTD 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 security target contains:

- visual (eye readable) biographical data and portrait of the holder,
- a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ),
- data elements on the MRTD's chip according to [ICAO-9303] for contactless machine reading.

The authentication of the traveler is based on the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and 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 trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of physical MRTD and logical MRTD as defined in §1.5.2.
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) [SS]. These security measures include the binding of the MRTD's chip to the passport book.

1.9 TOE Life-cycle

1.9.1 Four phases

The TOE life cycle is described in terms of the four life cycle phases:

Phase 1 "Development":
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.

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

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the nonvolatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 "Manufacturing":
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 in the nonvolatile non-programmable memories (ROM). The IC manufacturer 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 MRTD manufacturer has the following tasks:

- **Initialization:** adding the parts of the IC Embedded Software (NVM ES) to the EEPROM,
- **Pre-personalization:** creation of the MRTD application and equipping chip with Pre-personalization Data,
- **Inlay manufacturing:** packing the IC with hardware for the contactless interface.

The following tasks are not part of the TOE manufacturing:

- **Book manufacturing:** manufacturing the passport book.

The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 "Personalization of the MRTD":
The personalization of the MRTD includes:

- the survey of the MRTD holder biographical data,
- the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data),
- the printing of the visual readable data onto the physical MRTD,
- the writing the TOE User Data and TSF Data into the logical MRTD,
- configuration of the TSF if necessary.

The step "writing the TOE User Data" is performed by the Personalization Agent and includes but is not limited to the creation of:

- the digital MRZ data (EF.DG1),
- the digitized portrait (EF.DG2),
- the Document security object (SOD).

The signing of the Document security object by the Document signer [PKI] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 "Operational Use"
The TOE is used as MRTD's 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 used according to the security policy of the Issuing State but they can never be modified.

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

1.9.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	Infineon
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	Infineon
Initializer	Gemalto
Pre-personalizer	Gemalto
Inlay manufacturer	Gemalto
Book manufacturer	The entity agent who is acting on the behalf of the issuing State or Organization and manufactures the passport booklet that embeds the inlay.
Personalization Agent	The agent who is acting on the behalf of the issuing State or Organization and personalizes the MRTD for the holder by activities establishing the identity of the holder with biographic data.
MRTD Holder	The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.

Table 2 Identification of the actors

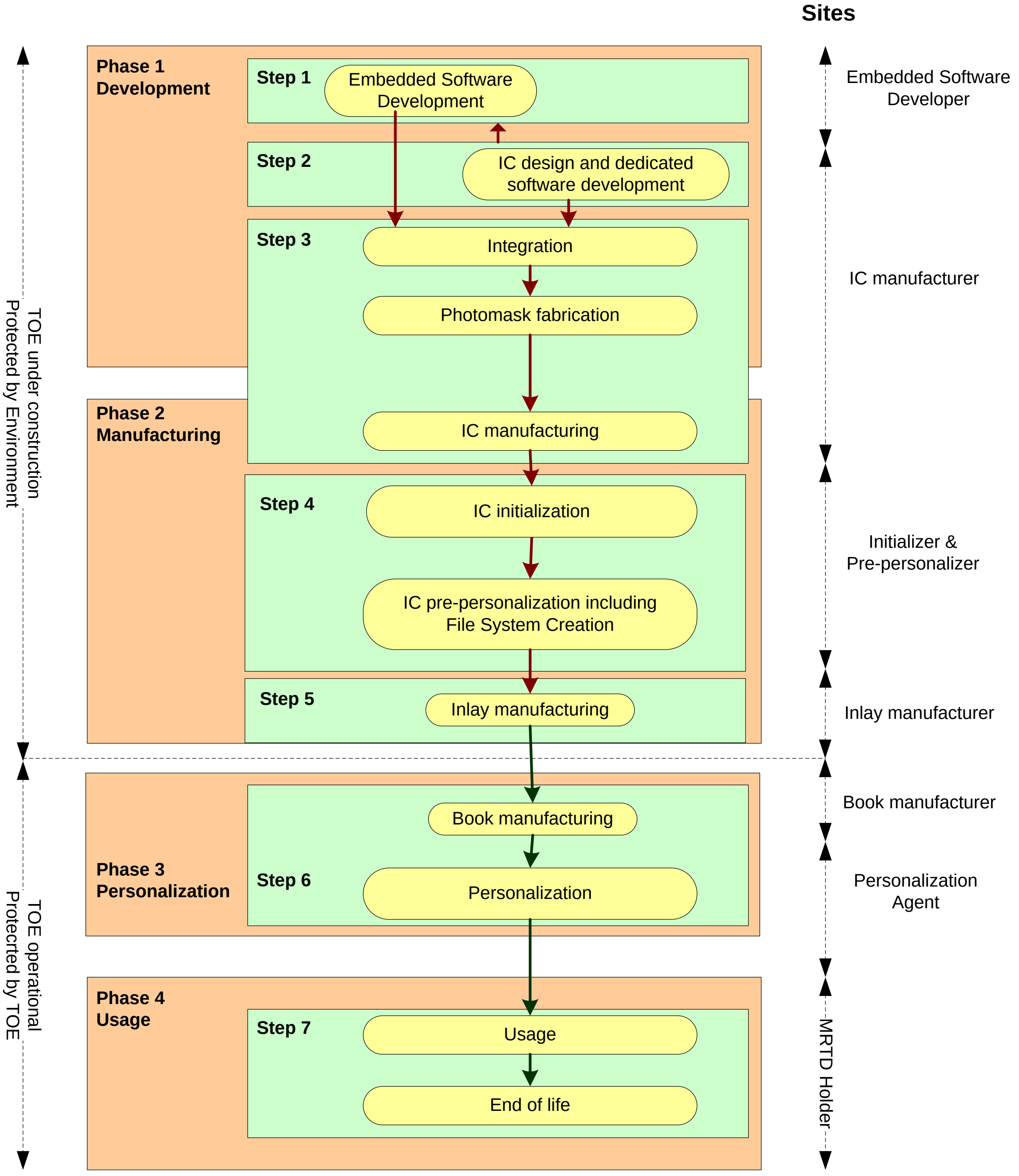

Figure 2 Lifecycle

Figure 2 describes the standard Life Cycle.

A module is manufactured at the IC manufacturer site. It is then shipped to Gemalto site where it is initialized and pre-personalized. Then the module is shipped to the Gemalto Inlay manufacturing site. The obtained inlay is then shipped to the book manufacturer and the Personalization agent. In the phases 1 and 2, the TOE is under construction and is protected by the development environment. In the phases 3 and 4, the TOE is operational and is protected by its security features.

Actors	Site
Integrated Circuit (IC) Developer	Described in the IC certificate [CR-IC]
Embedded Software Developer	Gemalto Singapore (for OS and Application) Gemalto Meudon, France (for Crytolibs)
Integrated Circuit (IC) Manufacturer	Described in the IC certificate [CR-IC]
Initializer & Pre-personalizer	Gemalto Gemenos, France Gemalto Singapore Gemalto Tczew, Poland
Inlay manufacturer	Gemalto Tczew, Poland

Table 3 TOE Development Environment

2 Conformance Claims

2.1 CC Conformance Claim

Common Criteria Version:

This security target conforms to CC version 3.1 r4 [CC-1][CC-2][CC-3]

Conformance to CCs part 2 and 3:

- Part 2 extended,
- Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, version 3.1 rev 4, September 2012, [CEM] has to be taken into account.

2.2 PP Claim

This security target claims strict conformance to the Protection Profile "Machine Readable Travel Document with ICAO Application, Basic Access Control" BSI-PP-0055 version 1.10 ([PP-MRTD-BAC]).

2.3 Package Claim

This security target is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 [CC-3] and evaluated under the terms of the SOG-IS agreement [SOG-IS].

2.4 Conformance statement

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

3 Security Problem Definition

3.1 Assets

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

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 [ICAO-9303]. 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.

Due to interoperability reasons as the 'ICAO Doc 9303' [ICAO-9303] the TOE described in this protection profile specifies only the BAC mechanisms with resistance against enhanced basic 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).

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.

3.2 Users / Subjects

This protection profile considers the following subjects:

Manufacturer

Generic term for the IC Manufacturer producing 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 manufacturing life cycle phase. The TOE itself does not distinguish between the IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

Personalization Agent

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 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 (iv) signing the Document Security Object defined in [ICAO-9303].

Terminal

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

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 contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic 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.

MRTD Holder

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

Traveler

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

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.

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.

T.Chip_ID

Identification of MRTD's chip

Adverse action: 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 contactless communication interface. Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance. Asset: Anonymity of user.

T.Skimming

Skimming the logical MRTD

Adverse action: An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance. Asset: confidentiality of logical MRTD data.

T.Eavesdropping

Eavesdropping to the communication between TOE and inspection system

Adverse action: An attacker is listening to an existing 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 printed on the MRTD data page but the attacker does not know these data in advance. Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance. Asset: confidentiality of logical MRTD data

T.Forgery

Forgery of data on MRTD's chip

Adverse action: 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 contactless chip. Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate MRTDs. Asset: authenticity of logical MRTD data

T.Abuse-Func

Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the MRTD holder. Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Information_Leakage

Information Leakage from MRTD's chip

Adverse action: 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 contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are 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). Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. Asset: confidentiality of logical MRTD and TSF data

T.Phys-Tamper

Physical Tampering

Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose 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) to 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. Threat agent: having enhanced basic attack potential, being in possession of a legitimate MRTD. Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Malfunction

Malfunction due to Environmental Stress

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

Application Note:

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

3.4 Organisational 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, sec. 3.2).

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-personalisation Data which contains at least the Personalisation Agent Key.

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.

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)3 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 Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [ICAO-9303].

Application Note:

The organizational security policy P.Personal_Data is drawn from the ICAO 'ICAO Doc 9303' [ICAO-9303]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

3.5 Assumptions

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

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).

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.

A.Pers_Agent

Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (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.

A.Insp_Sys

Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining a MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO-9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

A.BAC-Keys

Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [ICAO-9303], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

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.

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 [ICAO-9303] and the TSF data can be written by authorized Personalisation 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 personalisation. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

Application Note:

The OT.AC_Pers implies that

- The data of the LDS groups written during personalisation for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.
- 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.

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.

OT.Data_Conf

Confidentiality of personal 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 Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Application Note:

The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the 'ICAO Doc 9303' [ICAO-9303] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this protection profile. Thus the read access must be prevented even in case of a successful BAC Authentication.

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 Basic Inspection System or Personalization Agent.

Application Note:

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 Identification 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 contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

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 ICEmbedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

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.

Application Note:

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

OT.Prot_Phys-Tamper

Protection against Physical Tampering

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

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

OT.Prot_Malfunction

Protection against Malfunctions

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

Application Note:

A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2 Security Objectives for the Operational Environment

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.

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.

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.

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 all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303].

OE.BAC-Keys

Cryptographic quality of Basic Access Control Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [ICAO-9303] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

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 Basic 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 Basic Access Control [ICAO-9303].

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.

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 Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security Objectives Rationale

4.3.1 Threats

T.Chip_ID addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective OT.Identification by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

T.Skimming addresses the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf 'Confidentiality of personal data' through

Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment OE.BAC-Keys.

T.Eavesdropping addresses the reading of the logical MRTD trough the contactless interface or listening the communication between the MRTD's chip and a terminal. This threat is countered by the security objective OT.Data_Conf 'Confidentiality of personal data'.

T.Forgery addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective OT.AC_Pers 'Access Control for Personalization of logical MRTD' requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective OT.Data_Int 'Integrity of personal data' and OT.Prot_Phys-Tamper 'Protection against Physical Tampering'. The examination of the presented MRTD passport book according to OE.Exam_MRTD 'Examination of the MRTD passport book' shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Pass_Auth_Sign 'Authentication of logical MRTD by Signature' and verified by the inspection system according to OE.Passive_Auth_Verif 'Verification by Passive Authentication'.

T.Abuse-Func addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by OT.Prot_Abuse-Func 'Protection against Abuse of Functionality'. Additionally this objective is supported by the security objective for the TOE environment: OE.Personalization 'Personalization of logical MRTD' ensuring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

T.Information_Leakage is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against thesethreats is addressed by the directly related security objective OT.Prot_Inf_Leak 'Protection against Information Leakage'.

T.Phys-Tamper is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objective OT.Prot_Phys-Tamper 'Protection against Physical Tampering'.

T.Malfunction is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objective OT.Prot_Malfunction 'Protection against Malfunctions'.

4.3.2 Organisational Security Policies

P.Manufact requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by OT.Identification.

P.Personalization addresses the (i) the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment OE.Personalization 'Personalization of logical MRTD', and (ii) the access control for the user data and TSF data as described by the security objective OT.AC_Pers 'Access Control for Personalization of logical MRTD'. Note the manufacturer equips the TOE with the Personalization Agent Key(s) according to OT.Identification 'Identification and Authentication of the TOE'. The security objective OT.AC_Pers limits the management of TSF data and management of TSF to the Personalization Agent.

P.Personal_Data requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and (ii) enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives OT.Data_Int 'Integrity of personal data' describing the unconditional protection of the integrity of the stored data and during transmission. The security objective OT.Data_Conf 'Confidentiality of personal data' describes the protection of the confidentiality.

4.3.3 Assumptions

A.MRTD_Manufact is covered by the security objective for the TOE environment OE.MRTD_Manufact 'Protection of the MRTD Manufacturing' that requires to use security procedures during all manufacturing steps.

A.MRTD_Delivery is covered by the security objective for the TOE environment OE.MRTD_ Delivery 'Protection of the MRTD delivery' that requires to use security procedures during delivery steps of the MRTD.

A.Pers_Agent is covered by the security objective for the TOE environment OE.Personalization 'Personalization of logical MRTD' including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

A.Insp_Sys is covered by the security objectives for the TOE environment OE.Exam_MRTD 'Examination of the MRTD passport book'. The security objectives for the TOE environment

OE.Prot_Logical_MRTD 'Protection of data from the logical MRTD' will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

A.BAC-Keys is directly covered by the security objective for the TOE environment OE.BAC-Keys 'Cryptographic quality of Basic Access Control Keys' ensuring the sufficient key quality to be provided by the issuing State or Organization.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Chip_ID	OT.Identification, OE.BAC-Keys	Section 4.3.1
T.Skimming	OT.Data_Conf, OE.BAC-Keys	Section 4.3.1
T.Eavesdropping	OT.Data_Conf	Section 4.3.1
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRTD, OE.Passive_Auth_Verif, OE.Personalization	Section 4.3.1
T.Abuse-Func	OT.Prot_Abuse-Func, OE.Personalization	Section 4.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 4.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 4.3.1
T.Malfunction	OT.Prot_Malfunction	Section 4.3.1

Table 4 Threats and Security Objectives - Coverage

Security Objectives	Threats
OT.AC_Pers	T.Forgery
OT.Data_Int	T.Forgery
OT.Data_Conf	T.Skimming, T.Eavesdropping
OT.Identification	T.Chip_ID
OT.Prot_Abuse-Func	T.Abuse-Func
OT.Prot_Inf_Leak	T.Information_Leakage
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper
OT.Prot_Malfunction	T.Malfunction
OE.MRTD_Manufact	
OE.MRTD_ Delivery	
OE.Personalization	T.Abuse-Func, T.Forgery
OE.Pass_Auth_Sign	T.Forgery
OE.BAC-Keys	T.Chip_ID, T.Skimming
OE.Exam_MRTD	T.Forgery
OE.Passive_Auth_Verif	T.Forgery
OE.Prot_Logical_MRTD	

Table 5 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 4.3.2
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization	Section 4.3.2
P.Personal_Data	OT.Data_Conf, OT.Data_Int	Section 4.3.2

Table 6 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
OT.AC_Pers	P.Personalization
OT.Data_Int	P.Personal_Data
OT.Data_Conf	P.Personal_Data
OT.Identification	P.Manufact, P.Personalization
OT.Prot_Abuse-Func	
OT.Prot_Inf_Leak	
OT.Prot_Phys-Tamper	
OT.Prot_Malfunction	
OE.MRTD_Manufact	
OE.MRTD_ Delivery	
OE.Personalization	P.Personalization
OE.Pass_Auth_Sign	
OE.BAC-Keys	
OE.Exam_MRTD	
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	

Table 7 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	Section 4.3.3
A.MRTD_Delivery	OE.MRTD_ Delivery	Section 4.3.3
A.Pers_Agent	OE.Personalization	Section 4.3.3
A.Insp_Sys	OE.Exam_MRTD, OE.Prot_Logical_MRTD	Section 4.3.3
A.BAC-Keys	OE.BAC-Keys	Section 4.3.3

Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.MRTD_Manufact	A.MRTD_Manufact
OE.MRTD_ Delivery	A.MRTD_Delivery
OE.Personalization	A.Pers_Agent
OE.Pass_Auth_Sign	
OE.BAC-Keys	A.BAC-Keys
OE.Exam_MRTD	A.Insp_Sys
OE.Passive_Auth_Verif	
OE.Prot_Logical_MRTD	A.Insp_Sys

Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FAU_SAS - Audit Data Storage

5.1.1.1 Description

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.

5.1.1.2 Extended Components

Extended Component FAU_SAS.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

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.

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.2 Extended Family FCS_RND - Generation of Random Numbers

5.1.2.1 Description

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.

5.1.2.2 Extended Components

Extended Component FCS_RND.1

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

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.1.3 Extended Family FMT_LIM - Limited Capabilities and Availability

5.1.3.1 Description

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.

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.

5.1.3.2 Extended Components

Extended Component FMT_LIM.1

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 lifecycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

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.

FMT_LIM.1 Limited Capabilities

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].

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

Extended Component FMT_LIM.2

FMT_LIM.2 Limited Availability

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].

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited Capabilities.

5.1.4 Extended Family FPT_EMS - TOE Emanation

5.1.4.1 Description

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.

5.1.4.2 Extended Components

Extended Component FPT_EMS.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_EMS.1 TOE Emanation

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

6 Security Requirements

6.1 Security Functional Requirements

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

Definition of security attributes:

security attribute	Values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	Basic Inspection System	Terminal is authenticated as Basic Inspection System after successful Authentication in accordance with the definition in rule 2 of FIA_UAU.5.2.
	Personalisation Agent	Terminal is authenticated as Personalisation Agent after successful Authentication in accordance with the definition in rule 1 of FIA_UAU.5.2.

6.1.1 Class FAU Security Audit

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **Manufacturer** with the capability to store **IC Identification Data** in the audit records.

6.1.2 Class Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 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 **112 bit** that meet the following: **[ICAO-9303], normative appendix 5**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroing the RAM zone storing the key** that meets the following: **None**.

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS 180-4**.

FCS_COP.1/ENC Cryptographic operation

FCS_COP.1.1/ENC 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 **112 bit** that meet the following: **FIPS 46-3 [FIPS46-3] and [ICAO-9303], normative appendix 5, A5.3**.

FCS_COP.1/AUTH Cryptographic operation

FCS_COP.1.1/AUTH The TSF shall perform **symmetric authentication (encryption and decryption)** in accordance with a specified cryptographic algorithm **Triple-DES** and cryptographic key sizes **112 bit** that meet the following: **FIPS 46-3 [FIPS46-3]**.

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging - message authentication code**

in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bit** that meet the following: **ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)**.

6.1.3 Random Number Generation (FCS_RND.1)

FCS_RND.1 Quality Metric for Random Numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **K3 class of [AIS20] with seed entropy at least 112 bits and with strength of mechanism set to high**.

6.1.4 Class FIA Identification and Authentication

Application note: The following Table provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	Algorithms and key sizes according to [ICAO-9303], normative appendix 5, and [TG-EAC]
Basic Access Control Authentication Mechanism	FIA_UAU.4 and FIA_UAU.6	Triple-DES, 112 bit keys (cf. FCS_COP.1/ENC) and Retail-MAC, 112 bit keys (cf. FCS_COP.1/MAC)
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4	Triple-DES with 112 bit keys (cf. FCS_COP.1/AUTH)

FIA_UID.1 Timing of identification

FIA_UID.1.1 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",**
- **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.

FIA_UAU.1 Timing of authentication

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

- **Basic Access Control Authentication**
- **Mechanism,Authentication Mechanism based on Triple-DES**.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

- **Basic Access Control Authentication Mechanism**
- **Symmetric Authentication Mechanism based on Triple- DES**

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

- **the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanism(s): the Symmetric Authentication Mechanism with the Personalization Agent Key,**
- **the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys**.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 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**.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 1 to 10** unsuccessful authentication attempts occur related to **Unsuccessful Basic Access Control authentication attempt**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **block the Document Basic Access Keys**.

.

6.1.5 Class FDP User Data Protection

Application note: 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 Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 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**.

FDP_ACF.1 Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent,**
  - **Basic Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data EF.DG1 to EF.DG16 of the logical MRTD,**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes**
  - **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:

- **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,**
- **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 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 following additional rules:

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

FDP_UCT.1 Basic data exchange confidentiality

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

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **Basic Access Control SFP** 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.

6.1.6 Class FMT Security Management

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

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

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Initialization,**
- **Pre-personalization,**
- **Personalization**.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Manufacturer,**

- **Personalization Agent,**
- **Basic Inspection System**.

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

FMT_LIM.1 Limited Capabilities

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**

- **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**.

FMT_LIM.2 Limited Availability

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**

- **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**.

FMT_MTD.1/INI_ENA Management of TSF data

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

FMT_MTD.1/INI_DIS Management of TSF data

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**.

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys** to **the Personalization Agent**.

FMT_MTD.1/KEY_READ Management of TSF data

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

6.1.7 FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_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 architecture description' (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **electromagnetic radiation, variation of timing or power consumption** in excess of **intelligible threshold** enabling access to **Personalization Agent Key(s)** and **confidential User Data**.

FPT_FLS.1 Failure with preservation of secure state

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

- **Exposure to out-of-range operating conditions where therefore a malfunction could occur,**
- **failure detected by TSF according to FPT_TST.1**.

FPT_TST.1 TSF testing

FPT_TST.1.1 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 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**.

FPT_PHP.3 Resistance to physical attack

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.

6.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Objectives

6.3.1.1 Security Objectives for the TOE

OT.AC_Pers 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 BAC 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 [PP-MRTD-EAC] by using the symmetric authentication mechanism (FCS_COP.1/AUTH).

In case of using the BAC 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 Basic 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_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

OT.Data_Int 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 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 BAC 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 Basic Access Keys in a way that they cannot be read by anyone in accordance to FMT_MTD.1/KEY_READ.

OT.Data_Conf 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 blocks the Document Basic Access Key. 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 Basic 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 Basic Inspection System) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization for the key management for the Document Basic 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 Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 requests secure messaging after successful authentication of the terminal with Basic 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 Basic Access Keys.

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

OT.Identification 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 Basic 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 Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt. In case of failed authentication attempts FIA_AFL.1 blocks the Document Basic Access Key.

OT.Prot_Abuse-Func is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

OT.Prot_Inf_Leak 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_EMS.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

OT.Prot_Phys-Tamper is covered by the SFR FPT_PHP.3.

OT.Prot_Malfunction 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 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.AC_Pers	FPT_EMS.1, FCS_CKM.4, FCS_RND.1, FMT_MTD.1/KEY_READ, FMT_SMF.1, FIA_UAU.6, FIA_UAU.4, FIA_UAU.5, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FPT_PHP.3, FPT_FLS.1	Section 6.3.1
OT.Data_Int	FCS_RND.1, FMT_SMF.1, FCS_COP.1/SHA, FIA_UAU.6, FIA_UAU.4, FIA_UAU.5, FDP_UCT.1, FDP_UIT.1, FMT_SMR.1, FCS_CKM.1, FDP_ACC.1, FDP_ACF.1, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ	Section 6.3.1
OT.Data_Conf	FCS_CKM.4, FCS_RND.1, FMT_SMF.1, FIA_UAU.1, FIA_UAU.6, FIA_UAU.4, FIA_UAU.5, FDP_UCT.1, FDP_UIT.1, FMT_SMR.1, FCS_CKM.1, FIA_UID.1, FDP_ACC.1, FDP_ACF.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/MAC, FIA_AFL.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ	Section 6.3.1
OT.Identification	FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FIA_UID.1, FIA_AFL.1, FIA_UAU.1	Section 6.3.1
OT.Prot_Abuse-Func	FMT_LIM.1, FMT_LIM.2	Section 6.3.1
OT.Prot_Inf_Leak	FPT_EMS.1, FPT_TST.1, FPT_FLS.1, FPT_PHP.3	Section 6.3.1
OT.Prot_Phys-Tamper	FPT_PHP.3	Section 6.3.1
OT.Prot_Malfunction	FPT_TST.1, FPT_FLS.1	Section 6.3.1

Table 10 Security Objectives and SFRs - Coverage

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

Table 11 SFRs and Security Objectives

6.3.3 Dependencies

6.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FAU_SAS.1	No Dependencies	
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4, FCS_COP.1/ENC, FCS_COP.1/MAC
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4
FCS_COP.1/ENC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/AUTH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/MAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_RND.1	No Dependencies	
FIA_UID.1	No Dependencies	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FIA_UAU.4	No Dependencies	
FIA_UAU.5	No Dependencies	
FIA_UAU.6	No Dependencies	
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1
FDP_UCT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1
FDP_UIT.1	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_LIM.1	No Dependencies	
FMT_LIM.2	No Dependencies	
FMT_MTD.1/INI_ENA	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_WRITE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FPT_EMS.1	No Dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FPT_FLS.1	No Dependencies	
FPT_TST.1	No Dependencies	
FPT_PHP.3	No Dependencies	

Table 12 SFRs Dependencies

6.3.3.2 Rationale for the exclusion of Dependencies

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. The hash algorithm required by the SFR FCS_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS_CKM.1) nor an import (FDP_ITC.1/2) is necessary.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/AUTH is discarded. 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 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

The dependency FCS_CKM.4 of FCS_COP.1/AUTH is discarded. 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 or FDP_ITC. Since the key is permanently stored within the TOE there is no need for FCS_CKM.4, too.

The dependency FMT_MSA.3 of FDP_ACF.1 is discarded. 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.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1 is discarded. The SFR FDP_UCT.1 requires 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.

The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1 is discarded. The SFR FDP_UIT.1 requires 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.

6.3.3.3 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 13 SARs Dependencies

6.3.4 Rationale for the Security Assurance Requirements

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.

EAL 4 provides assurance by an analysis of the security functions, specifications, guidance, design of the TOE, and the implementation, to understand the security behaviour. The analysis is supported by independent testing of the security functions and an independent vulnerability analysis demonstrating resistance to penetration attackers.

EAL4 also provides assurance through the use of development environment controls and configuration management including automation, and evidence of secure delivery procedures.

6.3.5 ALC_DVS.2 Sufficiency of security measures

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.

7 TOE Summary Specification

7.1 TOE Summary Specification

The TOE being a composite product, the TOE Security Functionality is provided by both the Scosta embedded software (including the OS layers JKernel and Drivers) and by the IC.

7.1.1 TSFs provided by the Scosta embedded software

The following table provides the list of the security features provided by the embedded software

Security Feature	Description
SF.REL	Protection of data
SF.AC	Access control
SF_SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging

SF.REL

The SF.REL security feature provides the protection of data on the TOE. It includes:

- o physical protection of the TOE as defined in
  - ▪ FPT_PHP.3 to protect the TOE against physical attacks
  - ▪ FPT_EMS.1 to implement measures to limit information contained in electromagnetic and current emissions
  - ▪ FPT_FLS.1 to preserve secure states
- o the test mechanisms as defined in
  - ▪ FPT_TST.1 to preserve secure states
- o protection against misuse of tests as defined in
  - ▪ FMT_LIM.1 and FMT_LIM.2 to limit the capabilities and availability of the TSF after TOE delivery

SF.AC

The SF.AC security feature provides the access control of the TOE. It includes:

- o the access control by the terminal as defined in
  - ▪ FDP_ACC.1 and FDP_ACF.1 to enforce the access control mechanism
- o the access control to specific data as defined in
  - ▪ FAU_SAS.1 to provide initialization data accessible for reading and writing action to the pre-personaliser and the personaliser
  - ▪ FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ to restrict the ability for reading/writing of Initialization Data, Prepersonalization Data, Document Basic Access Keys and Personalization Agent Keys to the Manufacturer and the the Personalization Agent

- the role management as defined in
  - FMT_SMR.1 to maintain the different roles according to the life cycle status
- the management functions linked to the different states of the TOE as defined in
  - FMT_SMF.1 to maintain the different roles according to the life cycle status

SF.SYM_AUTH

The SF.SYM_AUTH security feature provides the symmetric authentication functions to the TOE. It includes:

- the identification and authentication as defined in
  - FIA_AFL.1 to detect unsuccessful authentication attempts with required consequences
  - 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 Basic Inspection Terminal and will stop communication after unsuccessful authentication attempt
  - FIA_UAU.4 to prevent reuse of authentication data to strengthen the authentication of the user
  - FIA_UAU.5 to enforce the TOE to accept the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys
  - FIA_UAU.6 to request secure messaging after successful authentication of the terminal with Basic Access Control Authentication Mechanism

SF.SM

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

- the secure transfer of data through SM as defined in
  - 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 cryptographic mechanisms used for the authentication and the SM, as defined in
  - FCS_CKM.1, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FIA_AFL.1 and FCS_RND.1. Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function
  - the erasure of session keys as defined in FCS_CKM.4

7.1.2 TSF provided by the Security IC

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IC]. The IC and its primary embedded software have been evaluated at level EAL 5+. The following table presents the list of security features provided by the IC.

Security Feature	Description
SF_DPM	Device phase management
SF_PS	Protection against snooping
SF_PMA	Protection against modifying attacks
SF_PLA	Protection against logical attacks
SF_CS	Cryptographic support

These SF are described in [ST-IC].

7.2 SFRs and TSS

7.2.1 *Association tables of SFRs and TSS*

Security Functional Requirements	TOE Summary Specification
FAU_SAS.1	SF.AC
FCS_CKM.1	SF.SM
FCS_CKM.4	SF.SM
FCS_COP.1/SHA	SF.SM
FCS_COP.1/ENC	SF.SM
FCS_COP.1/AUTH	SF.SM
FCS_COP.1/MAC	SF.SM
FCS_RND.1	SF.SM
FIA_UID.1	SF.SYM_AUTH
FIA_UAU.1	SF.SYM_AUTH
FIA_UAU.4	SF.SYM_AUTH
FIA_UAU.5	SF.SYM_AUTH
FIA_UAU.6	SF.SYM_AUTH
FIA_AFL.1	SF.SYM_AUTH, SF.SM
FDP_ACC.1	SF.AC
FDP_ACF.1	SF.AC
FDP_UCT.1	SF.SM
FDP_UIT.1	SF.SM
FMT_SMF.1	SF.AC
FMT_SMR.1	SF.AC
FMT_LIM.1	SF.REL
FMT_LIM.2	SF.REL
FMT_MTD.1/INI_ENA	SF.AC
FMT_MTD.1/INI_DIS	SF.AC
FMT_MTD.1/KEY_WRITE	SF.AC
FMT_MTD.1/KEY_READ	SF.AC
FPT_EMS.1	SF.REL
FPT_FLS.1	SF.REL
FPT_TST.1	SF.REL
FPT_PHP.3	SF.REL

Table 14 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.REL	FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3
SF.AC	FAU_SAS.1, FDP_ACC.1, FDP_ACF.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ
SF.SYM_AUTH	FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_AFL.1
SF.SM	FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/ENC, FCS_COP.1/AUTH, FCS_COP.1/MAC, FCS_RND.1, FIA_AFL.1, FDP_UCT.1, FDP_UIT.1

Table 15 TSS and SFRs - Coverage

8 Rationale for Composite Product

This Section provides the justifications for the compatibility between this security target and the IC security target [ST-IC].

8.1 Compatibility on the security environment

8.1.1 Threats

T.Chip_ID, T.Skimming, T.Eavesdropping are specific to the ScostaCL Embedded Software and do not have conflict with the threats of [ST-IC].

T.Forgery is included in T.Phys-Manipulation of [ST-IC].

T.Abuse-Func is included in T.Abuse-Func of [ST-IC].

T.Information_Leakage is included in T.Leak-Inherent and T.Leak-Forced of [ST-IC].

T.Phys-Tamper is included in T.Phys-Manipulation of [St-IC].

T.Malfunction is included in T.Malfunction of [ST-IC].

As a result, the threats of this security target do not contradict [ST-IC].

8.1.2 OSP

P.Manufact, P.Personalization and P.PersonalData do not have conflict with the OSP of [ST-IC].

As a result, the OSP of this security target does not contradict [ST-IC].

8.1.3 Assumptions

A.MRTD_Manufact and A.MRTD_Delivery are included in A.Process-Sec-IC of [ST-IC].

A.Pers_Agent, A.Insp_Sys, and A.BAC-Keys do not have conflict with the assumptions of [ST-IC].

As a result, the assumptions for the environment of this security target do not contradict [ST-IC].

8.2 Compatibility on the security objectives

8.2.1 Objectives for the TOE

OT.AC_Pers does not have conflict with the objectives of [ST-IC].

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

OT.Data_Conf does not have conflict with the objectives of [ST-IC].

OT.Identification is included in O.Identification of [ST-IC].

OT.Prot_Abuse-Func is included in O.Abuse-Func of [ST-IC].

OT.Prot_Inf_Leak is included in O.Leak-Inherent and O.Leak-Forced of [ST-IC].

OT.Prot_Phys-Tamper is included in O.Phys-Manipulation of [ST-IC].

OT.Prot_Malfunction is included in O.Malfunction of [ST-IC].

As a result, the objectives for the TOE of this security target do not contradict [ST-IC].

8.2.2 Objectives for the environment

OE.MRTD_Manufact is included in OE.Process-Sec-IC of [ST-IC].

OE.MRTD_ Delivery is included in OE.Process-Sec-IC [ST-IC].

OE.Personalization is partly included in OE.Process-Sec-IC [ST-IC].

OE.Pass_Auth_Sign, OE.BAC_Keys, OE.Exam_MRTD, OE.Passive_Auth_Verif, OE.Prot_Logical_MRTD are specific to MRTD and do not have conflict with the objectives of [ST-IC].

As a result, the objectives for the environment of this security target do not contradict [ST-IC].

8.3 Compatibility on the SFRs

The Security Functional Requirements present in the IC Security Target are relevant to this Security Target.

Relevant:

FAU_SAS.1 matches FAU_SAS.1 of [ST-IC].

FCS_RND.1, FCS_CKM.1 and FCS_COP.1 are supported by FCS_CKM.1, FCS_COP.1 and FCS_RNG.1 of [ST-IC].

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

FPT_FLS.1 matches FPT_FLS.1 of [ST-IC].

FPT_TST.1 matches FPT_TST.2 of [ST-IC].

FDP_ACC.1, FDP_ACF.1: no interaction and contradiction between the application and the chip SFRs as FDP_ACC.1 and FDP_ACF.1 of [ST-IC] concern memory access control policy (IC).

FMT_SMF.1: no interaction and contradiction between the application and the chip SFRs as FMT_SMF.1 of [ST-IC] concerns memory management unit.

FMT_LIM.1, FMT_LIM.2 are included in FMT_LIM.1 and FMT_LIM.2 of [ST-IC]. These SFR are about not disclosing or manipulating data after delivery.

FCS_CKM.4, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_AFL.1, FDP_ACC.1, FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, and FPT_TST.1 are specific to MRTD BAC and they do not have conflict with [ST-IC].

Not relevant

FMT_MSA.3, FMT_MSA.1, FDP_SDI.1, FDP_SDI.2, FRU_FLT.2, FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 of [ST-IC] do not concern the application thus they are not relevant for this composition.

As a result, the SFR of this security target do not contradict [ST-IC].

8.4 Compatibility on the Security Functionality

SF.REL, SF.AC, SF.SYM_AUTH and SF.SM do not contradict the IC security features described in [ST-IC].

Relevant:

SF.AC is supported by SF_DPM of [ST-IC].

SF.REL is supported by SF_PS, SF_PMA, and SF_PLA of [ST-IC].

SF.SM is supported by SF_CS of [ST-IC].SF.SYM_AUTH is specific to MRTD BAC and it does not have conflict with [ST-IC].