



Security Target

SOMA_80IFX Electronic Passport

Version 1.0.0

Common Criteria – ISO/IEC 15408 EAL 4+

Certification ID: BSI-DSZ-CC-0498



Revision History

| Version | Date | Author | Revision Description |
|---------|------------|--------|----------------------|
| 1.0.0 | 05/10/2009 | Gep | First public release |

1 Document Overview

1.1 Tables

1.1.1 Table of Contents

| | | |
|-------|--|----|
| 1 | Document Overview | 3 |
| 1.1 | Tables..... | 3 |
| 1.1.1 | Table of Contents | 3 |
| 1.1.2 | List of Tables | 4 |
| 1.1.3 | List of Figures..... | 5 |
| 1.2 | Acronyms, Glossary and Notations | 5 |
| 1.2.1 | Acronyms | 5 |
| 1.3 | Glossary | 6 |
| 1.4 | Technical References..... | 11 |
| 2 | ST Introduction..... | 14 |
| 2.1 | ST Overview | 14 |
| 2.2 | ST Identification..... | 14 |
| 2.3 | CC Conformance..... | 14 |
| 2.4 | Statement of Compatibility concerning Composite Security Target..... | 15 |
| 3 | TOE Description..... | 16 |
| 3.1 | TOE Definition | 16 |
| 3.2 | TOE Boundaries | 16 |
| 3.3 | TOE Usage..... | 19 |
| 3.4 | TOE Security Features | 20 |
| 3.5 | TOE Life-cycle..... | 21 |
| 3.5.1 | Development | 22 |
| 3.5.2 | Manufacturing..... | 23 |
| 3.5.3 | Personalization of the MRTD..... | 23 |
| 3.5.4 | Operational Use | 24 |
| 3.5.5 | Terminated | 24 |
| 4 | TOE Security Environment..... | 25 |
| 4.1 | Introduction..... | 25 |
| 4.1.1 | Assets | 25 |
| 4.1.2 | Subjects..... | 25 |
| 4.2 | Assumptions | 27 |
| 4.3 | Threats | 27 |
| 4.4 | Organizational Security Policies | 30 |
| 5 | Security Objectives | 31 |
| 5.1 | TOE Security Objectives | 31 |
| 5.2 | Environment Security Objectives..... | 33 |
| 5.2.1 | Development and Manufacturing Environment..... | 33 |
| 5.2.2 | Operational Environment..... | 34 |
| 6 | IT Extended Components Definition..... | 36 |
| 6.1 | Definition of the FAU_SAS Family..... | 36 |
| 6.2 | Definition of the FCS_RND Family | 36 |



- 6.3 Definition of the FIA_API Family 37
- 6.4 Definition of the FMT_LIM Family 38
- 6.5 Definition of the FPT_EMSEC Family 40
- 7 IT Security Requirements 42
 - 7.1 Security Functional Requirements for the TOE 42
 - 7.1.1 Class FAU Security Audit 42
 - 7.1.2 Class Cryptographic Support (FCS) 42
 - 7.1.3 Class FIA Identification and Authentication 45
 - 7.1.4 Class FDP User Data Protection 49
 - 7.1.5 Class FMT Security Management 52
 - 7.1.6 Class FPT Protection of the Security Functions 56
 - 7.2 Security Assurance Requirements for the TOE 60
 - 7.3 Security Requirements for the IT environment 60
 - 7.3.1 Passive Authentication 60
 - 7.3.2 Personalization Terminals 61
 - 7.3.3 Administration Terminals 64
 - 7.3.4 Basic Inspection Systems 65
- 8 TOE Summary Specification 69
 - 8.1 TOE Security Functions 69
 - 8.1.1 SF1 69
 - 8.1.2 SF2 69
 - 8.1.3 SF3 70
 - 8.1.4 SF4 70
 - 8.1.5 SF5 70
 - 8.1.6 SF6 70
 - 8.2 SOF claim for TSF 71
 - 8.3 Assurance Measures 72
- 9 Protection Profile Claims 73
- 10 Rationale 74
 - 10.1 Security Objectives Rationale 74
 - 10.2 Security Requirements Rationale 77
 - 10.2.1 Security Objectives for the TOE 77
 - 10.2.2 Security Objectives for the IT Environment 82
 - 10.3 Dependency Rationale 84
 - 10.4 Security Assurance Requirements Rationale 88
 - 10.5 Security Requirements – Mutual Support and Internal Consistency 89

1.1.2 List of Tables

- Table1: ST Identification 14
- Table2: FAU_SAS Family 36
- Table3: FCS_RND Family 37
- Table4: FIA_API Family 38
- Table5: FMT_LIM Family 39
- Table6: FPT_EMSEC Family 41
- Table7: Authentication Mechanisms 45
- Table8: FIA_AFL.1 Refinement 46
- Table9: Assurance Requirements documentation 72
- Table10: Security Objectives Rationale 74

| | |
|--|----|
| Table11: Security Objectives Coverage for the TOE by the SFR | 78 |
| Table12: Security Objectives Coverage for the IT Environment by the SFR..... | 83 |
| Table13: Dependencies between the SFR for the TOE | 86 |
| Table14: Dependencies between the SFR for the IT Environment | 88 |

1.1.3 List of Figures

| | |
|------------------------------|----|
| Figure1: Physical TOE | 17 |
| Figure2: Logical TOE | 18 |
| Figure3: TOE Life Cycle..... | 22 |

1.2 Acronyms, Glossary and Notations

1.2.1 Acronyms

| | |
|----------------------------|--|
| AID | Application Identifier (ISO 7816) |
| AK_{PA} | Personalization Agent Key Pair |
| ATS | Answer to Select |
| BAC | Basic Access Control |
| BIS | Basic Inspection System |
| C_{DS} | DS Public Key Certificate |
| CBC | Cipher-block Chaining (block cipher mode of operation) |
| CC | Common Criteria |
| COM | Common data group of the LDS (ICAO TR-LDS) |
| CPS | Common Personalization Standard |
| CPU | Central Processing Unit |
| CSCA | Country Signing Certification Authority |
| CSN | Chip Security Number |
| DF | Dedicated File (ISO 7816) |
| DG | Data Group (ICAO TR-LDS) |
| DPA | Differential Power Analysis |
| DS | Document Signer |
| ECB | Electronic Codebook (block cipher mode of operation) |
| EEPROM | Electrically Erasable Read Only Memory |
| EF | Elementary File (ISO 7816) |
| EIS | Extended Inspection System |
| IC | Integrated Circuit |
| ICCSN | IC Chip Serial Number |
| IS | Inspection System |
| K_{ENC_BAC} | BAC Encryption Key |
| K_{MAC_BAC} | BAC MAC Key |
| KPr_{CSCA} | CSCA Private Key |
| KPr_{DS} | DS Private Key |
| LDS | Logical Data Security |
| LCS | Life Cycle Status |
| MAC | Message Authentication Code |
| MED | Memory Encryption and Decryption unit |
| MF | Master File (ISO 7816) |
| MMU | Memory Management Unit |
| MRTD | Machine Readable Travel Document |
| MRZ | Machine Readable Zone |

| | |
|-----------------------|--|
| NMI | Non Maskable Interrupt |
| NTWG | New Technology Working Group (ICAO) |
| OCR | Optical Character Recognition |
| OS | Operating System |
| OSP | Organization Security Policy |
| PICC | Proximity Integrated Circuit Chip |
| PIS | Primary Inspection System |
| PP | Protection Profile |
| PROM | Programmable Read Only Memory |
| PUPI | Pseudo-Unique PICC Identifier |
| RAM | Random Access Memory |
| RND.ICC | ICC Random (used in BAC) |
| RNG | Random Number Generator |
| ROM | Read Only Memory |
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |
| SO_D | Document Security Object |
| SOF | Strength of Function |
| SPA | Simple Power Analysis |
| ST | Security Target |
| TDES | Triple DES |
| TOE | Target of Evaluation |
| TSC | TOE Scope of Control |
| TSF | TOE Security Functions |
| TR | Technical Report |
| TR-LDS | TR published by ICAO which defines the LDS |
| TR-PKI | TR published by ICAO which defines SO _D and the BAC mechanism |
| VIZ | Visual Inspection Zone |

1.3 Glossary

| | |
|--------------------------------|--|
| <i>Active Authentication</i> | Security mechanism defined in TR-PKI [R16] 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 or organization. |
| <i>application note</i> | Additional information that is considered relevant or useful for the construction, evaluation, or use of the TOE. |
| <i>audit records</i> | Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data. |
| <i>authenticity</i> | Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the Issuing State or Organization. |
| <i>Basic Access Control</i> | Security mechanism defined by ICAO [R16] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with the Document BAC Keys. |
| <i>Basic Inspection System</i> | An inspection system which implements the terminals part of the BAC Mechanism and authenticates themselves to the MRTD's chip using the Document BAC Keys derived form |

| | |
|--|--|
| <i>biographical data</i> | the printed MRZ data for reading the logical MRTD. The personalized details of the bearer of the document appearing as text in the VIZ and MRZ on the biographical data page of a passport book or on a travel card or visa [R13]. |
| <i>biometric reference data</i> | Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data. |
| <i>counterfeit</i> | An unauthorized copy or reproduction of a genuine security document made by whatever means [R13]. |
| <i>Country Signing Certification Authority</i> | Certification Authority of the Issuing State or Organization which attests the validity of certificates and digital signatures issued by the Document Signer. |
| <i>Document Basic Access Keys</i> | Pair of symmetric TDES keys used for secure messaging with encryption (K_{ENC_BAC}) and message authentication (K_{MAC_BAC}) of data transmitted between the MRTD's chip and the inspection system [R16]. It is derived from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book. |
| <i>Document Security Object</i> | A RFC3369 CMS Signed Data Structure, signed by the Document Signer. Carries the hash values of the LDS DG's and is stored in the MRTD's chip. It may carry the Document Signer Certificate (C_{DS}) [R16]. |
| <i>Document Signer</i> | Entity delegated by the Issuing State or Organization to digitally sign the DG's present in the LDS. |
| <i>eavesdropper</i> | A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip. |
| <i>enrolment</i> | The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity [R14]. |
| <i>Extended Access Control</i> | Security mechanism identified in TR-PKI [R16] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Keys and to get write and read access to the logical MRTD and TSF data. |
| <i>Extended Inspection System</i> | A role of a terminal as part of an inspection system which is in addition to the BIS authorized by the Issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism. |
| <i>Forgery</i> | Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait [R13]. |
| <i>Global interoperability</i> | The capability of inspection systems (either manual or automated) in different States throughout the world to |

| | |
|---|---|
| | <p>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.</p> |
| <i>impostor</i> | <p>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 [R13].</p> |
| <i>Initialization Data</i> | <p>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).</p> |
| <i>inspection</i> | <p>The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity.</p> |
| <i>Inspection System</i> | <p>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.</p> |
| <i>Integrated Circuit</i> | <p>Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.</p> |
| <i>integrity</i> | <p>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</p> |
| <i>Issuing Organization</i> | <p>Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer) [R15].</p> |
| <i>Issuing State</i> | <p>The Country issuing the MRTD [R15].</p> |
| <i>Logical Data Structure</i> | <p>The collection of groupings of DG's stored in the optional capacity expansion technology [R15]. The capacity expansion technology used is the MRTD's chip.</p> |
| <i>Logical MRTD</i> | <p>Data of the MRTD holder stored according to the LDS [R15] as specified by ICAO on the contactless IC. It presents contactless readable data including (but not limited to):</p> <ol style="list-style-type: none">i. personal data of the MRTD holderii. the digital Machine Readable Zone Data (digital MRZ data, DG1),iii. the digitized portraits (DG2),iv. the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both andv. the other data according to LDS (DG5 to DG16). |
| <i>Machine Readable Travel Document</i> | <p>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 [R15].</p> |
| <i>Machine Readable Zone</i> | <p>Fixed dimensional area located on the front of the MRTD</p> |

| | |
|--|--|
| | 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 [R15]. |
| <i>machine-verifiable feature</i> | <i>biometrics</i> 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. |
| <i>MRTD Administrator</i> | The entity delegated by the Issuing State or Organization to administer the MRTD once it has been issued. Its duties may include the following: <ul style="list-style-type: none">i. terminating MRTD's,ii. adding new DG's to the LDS of an MRTD (modifying the SO_D and COM so as to reflect the new DG's) |
| <i>MRTD application</i> | Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: <ul style="list-style-type: none">i. the file structure implementing the LDS [R15],ii. the definition of the User Data, but does not include the User Data itself (i.e. content of DG1 to DG14 and DG 16) andiii. the TSF Data including the definition the authentication data but except the authentication data itself. |
| <i>MRTD Basic Access Control</i> | 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. |
| <i>MRTD holder</i> | The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD. |
| <i>MRTD's chip</i> | A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the LDS [R15]. |
| <i>MRTD's chip Embedded Software</i> | 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. |
| <i>Optional biometric reference data</i> | Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (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. |
| <i>Passive Authentication</i> | Passive Authentication is a mechanism that ensures the authenticity of the DG's present in the LDS by: <ul style="list-style-type: none">i. the verification of the digital signature of the SO_D andii. comparing the hash values of the read LDS data fields with the hash values contained in the SO_D. |
| <i>Personalization</i> | The process by which the portrait, signature and biographical data are applied to the document [R13]. |

| | |
|---|--|
| <i>Personalization Agent</i> | The agent delegated by the Issuing State or Organization to personalize the MRTD for the holder by <ol style="list-style-type: none">establishing the identity the holder for the biographic data in the MRTD,enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or the encoded iris image(s) andwriting these data on the physical and logical MRTD for the holder. |
| <i>Personalization Agent Authentication Information</i> | TSF data used for authentication proof and verification of the Personalization Agent. |
| <i>Physical travel document</i> | Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): <ol style="list-style-type: none">biographical data,data of the MRZ,photographic image andother data. |
| <i>Pre-personalization Data</i> | Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair (AK _{PA}). |
| <i>Pre-personalized MRTD's chip</i> | MRTD's chip equipped with an unique identifier, the AK _{PA} , and an unique asymmetric Active Authentication Key Pair of the chip. |
| <i>Primary Inspection System</i> | A 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. |
| <i>Receiving State</i> | The Country to which the MRTD holder is applying for entry [R15]. |
| <i>reference data</i> | 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. |
| <i>secondary image</i> | A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. |
| <i>secure messaging</i> | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [R17]. |
| <i>skimming</i> | 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. |
| <i>travel document</i> | 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. |
| <i>traveler</i> | Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder. |
| <i>TSF data</i> | Data created by and for the TOE, that might affect the operation of the TOE [R6]. |
| <i>Unpersonalized MRTD</i> | MRTD material prepared to produce an personalized MRTD containing an initialized and pre-personalized MRTD's chip. |

| | |
|--------------------------|---|
| <i>User data</i> | Data created by and for the user, that does not affect the operation of the TSF [R6]. |
| <i>Verification</i> | 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 [R14]. |
| <i>Verification data</i> | 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. |

1.4 Technical References

- [R1] **BSI AIS31**: *Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001*
- [R2] **BSI**: *Certification Report BSI-DSZ-CC-0399-2007 for Infineon Smart Card IC (Security Controller) SLE66CLX800PE/m1581-e12*
- [R3] **BSI PP-002-2001**: *Protection Profile conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001*
- [R4] **BSI PP-0017-2005**: *Protection Profile Machine Readable Travel Document with „ICAO Application“, Version 1.0, BSI-PP-0017, 2005-08-18*
- [R5] **BSI**: *Technical Report Advanced Security Mechanisms for Machine Readable Travel Documents, Version 0.8 (final)*
- [R6] **CC 1**: *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-001*
- [R7] **CC 2**: *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, August 2005, version 2.3, CCMB-2005-08-002*
- [R8] **CC 3**: *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 2005, version 2.3, CCMB-2005-08-003*
- [R9] **EMV CPS**: *EMV Card Personalization Specification – version 1.0, June 2003*

- [R10] **FIPS 46-3:** *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology*
- [R11] **FIPS 180-2:** *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 180-2, SECURE HASH STANDARD, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology – 2002 August 1*
- [R12] **GlobalPlatform:** *GlobalPlatform Card Specification – version 2.1.1, March 2003*
- [R13] **ICAO Doc 9303:** *MACHINE READABLE TRAVEL DOCUMENTS – Part 3 Machine Readable Official Travel Documents Volume 2 Specifications for Electronically Enabled Official Travel Documents with Biometric Identification Capability Approved by the Secretary General and published under his authority – Third Edition – 2006*
- [R14] **ICAO TR-BD:** *Biometrics Deployment of MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using MRTD's; Version 2.0*
- [R15] **ICAO TR-LDS:** *MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: Development of a LOGICAL DATA STRUCTURE for Optional Capacity Expansion Technologies; Version 1.7*
- [R16] **ICAO TR-PKI:** *MACHINE READABLE TRAVEL DOCUMENTS – Technical Report: PKI for MRTD offering ICC Read-only Access; Version 1.1*
- [R17] **ISO/IEC 7816-4:** *Identification cards – Integrated circuit cards. Part 4: Organization, security and commands for interchange. Second edition 2005-01-15*
- [R18] **ISO/IEC 9796-2 2002:** *Information Technology – Security Techniques – Digital Signature Scheme – Part 2: Integer factorization based mechanism, 2002*
- [R19] **ISO/IEC 9797-1 1999:** *Information Technology – Security Techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher, 1999*
- [R20] **ISO/IEC 11568-2 2005:** *Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle*
- [R21] **Gep:** *Functional Specification for SOMA_80IFX e-Passport*
- [R22] **Gep:** *High-Level Design of SOMA_80IFX software embedded*

- [R23] **Infineon Technologies AG:** *Security and Chipcard ICs - SLE66CLX800PE/m1581-e12 - version 1.3*

- [R24] **ISO/IEC:** *International Standard 14443-1 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 1: Physical characteristics*

- [R25] **ISO/IEC:** *International Standard 14443-2 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 2: Radio frequency interface power and signal interface*

- [R26] **ISO/IEC:** *International Standard 14443-3 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 3: Initialization and anticollision*

- [R27] **ISO/IEC:** *International Standard 14443-4 - Identification cards – Contactless Integrated circuit cards – Proximity cards. Part 4: Transmission protocol*

2 ST Introduction

2.1 ST Overview

This Security Target (ST) document defines the security objectives and requirements for the SOMA_80IFX product. This product has an Operating System (OS) masked onto the Read Only Memory (ROM) of an Integrated Circuit (IC) chip with a radiofrequency (contactless) interface. SOMA_80IFX is utilized by Machine Readable Travel Documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO) and addresses the advanced security methods Basic Access Control (BAC) in the Technical Reports (TR) of the ICAO New Technology Working Group (NTWG). The Target of Evaluation (TOE) is used in the context of the ICAO application as described in the Protection Profile (PP) [R4].

2.2 ST Identification

| | |
|----------------------------|---|
| TOE | SOMA_80IFX |
| TOE Version | 1.1.0 |
| ST Title | Security Target Lite SOMA_80IFX Electronic Passport |
| ST Version | 1.0.0 |
| Protection Profile | BSI-PP-0017-2005 |
| Evaluation Criteria | Common Criteria version 2.3 compliant with ISO 15408:2005 |
| Evaluation Level | EAL 4 + ADV_IMP.2 and ALC_DVS.2 |
| Certification ID | BSI-DSZ-CC-0498 |
| Developer | Gep S.p.A. |

Table1: ST Identification

2.3 CC Conformance

The security target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Introduction and general model, August 2005, version 2.3, CCMB-2005-08-002 (extended)

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 2005, version 2.3, CCMB-2005-08-003 (conformant)

The target certification is conformant to EAL4 augmented with ADV_IMP.2 and ALC_DVS.2.

2.4 Statement of Compatibility concerning Composite Security Target

- This composite security target trusts in and relies on the security target of the underlying hardware [R23] Infineon - SLE66CLX800PE with certification ID: BSI-DSZ-CC-399-2007.

3 TOE Description

3.1 TOE Definition

The TOE is the proximity integrated circuit chip (PICC) of the MRTD chip programmed according to the Logical Data Structure (LDS) [R15] with the following functionality:

- BAC mechanism according to the ICAO TR-PKI [R16]
- Specific administrative commands for the management of the TOE during the Operational Use phase.

The TOE is comprised of:

- the circuitry of the MRTD's chip (IC produced by *Infineon* - SLE66CLX800PE with certification ID: BSI-DSZ-CC-399-2007);
- antenna connected to the IC embedded in a substrate;
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
- the IC Embedded Software (SOMA_80IFX OS);
- the MRTD application – LDS;
- the associated technical documentation (Administrator and User Guide).

3.2 TOE Boundaries

The **physical** structure of the SOMA_80IFX product is comprised of the following:

- an integrated circuit chip (SLE66CLX800PE Infineon microcontroller certified) powered by the electromagnetic field radiated by the inspection system including the following:
 - a dedicated CPU,
 - a crypto co-processor including a 112 bit dual key DES accelerator,
 - 240 Kbyte of non-volatile read-only memory (ROM) to hold the operating system,
 - 7100 byte of volatile programmable memory (RAM),
 - 256 bytes of internal RAM (IRAM),

- 80 Kbyte of non-volatile, readable and writable memory (EEPROM), to hold the file system and additions to the operating system;
 - a memory control unit (MCU) that distributes data to and from memory components; it includes a FCURSE module for camouflage of access operations;
 - Memory Encryption and Decryption Unit (MED);
 - Memory Management Unit (MMU),
 - Security sensors,
 - Checksum module (CRC),
 - Interrupt module (INT),
 - Timer,
 - A radiofrequency interface for contactless communications,
 - ISO/IEC 7816 and 14443 type A and B interfaces,
 - Random Number Generator (RNG).
- contactless interface (antenna),
 - substrate containing the antenna and the chip.

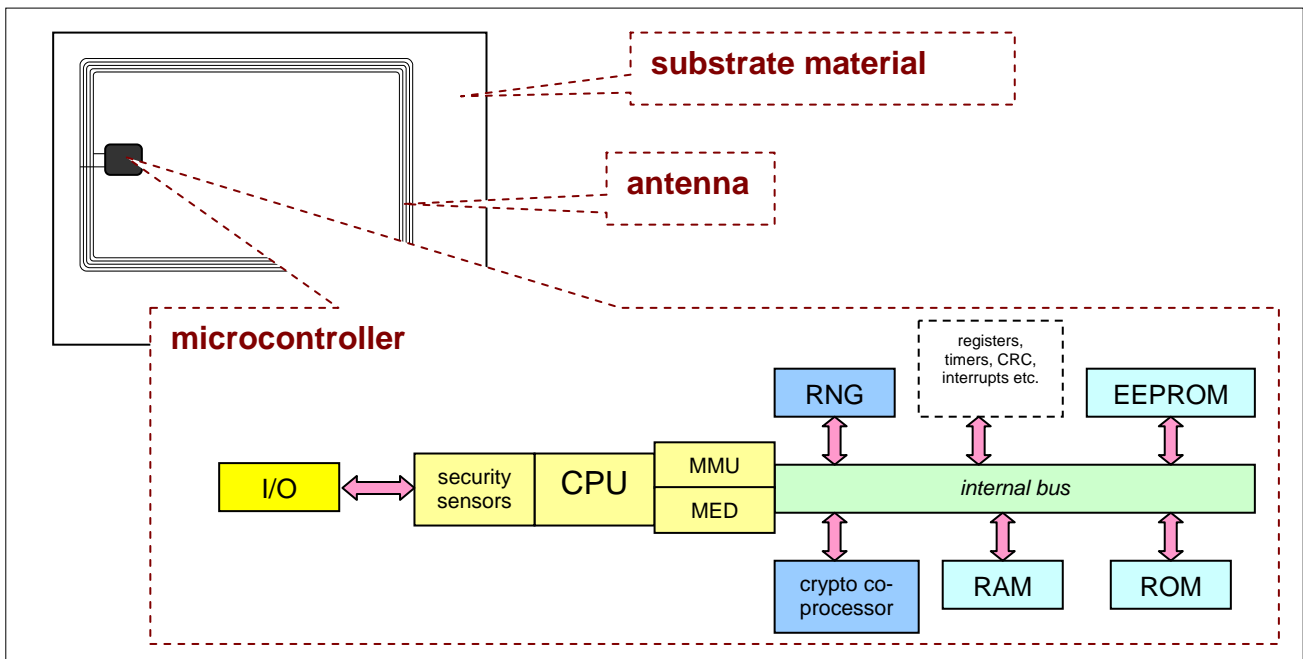


Figure1: Physical TOE

Therefore, the *SOMA_80IFX e-Passport* product delivered is an inlay that the Personalization Agent will incorporate into the MRTD.

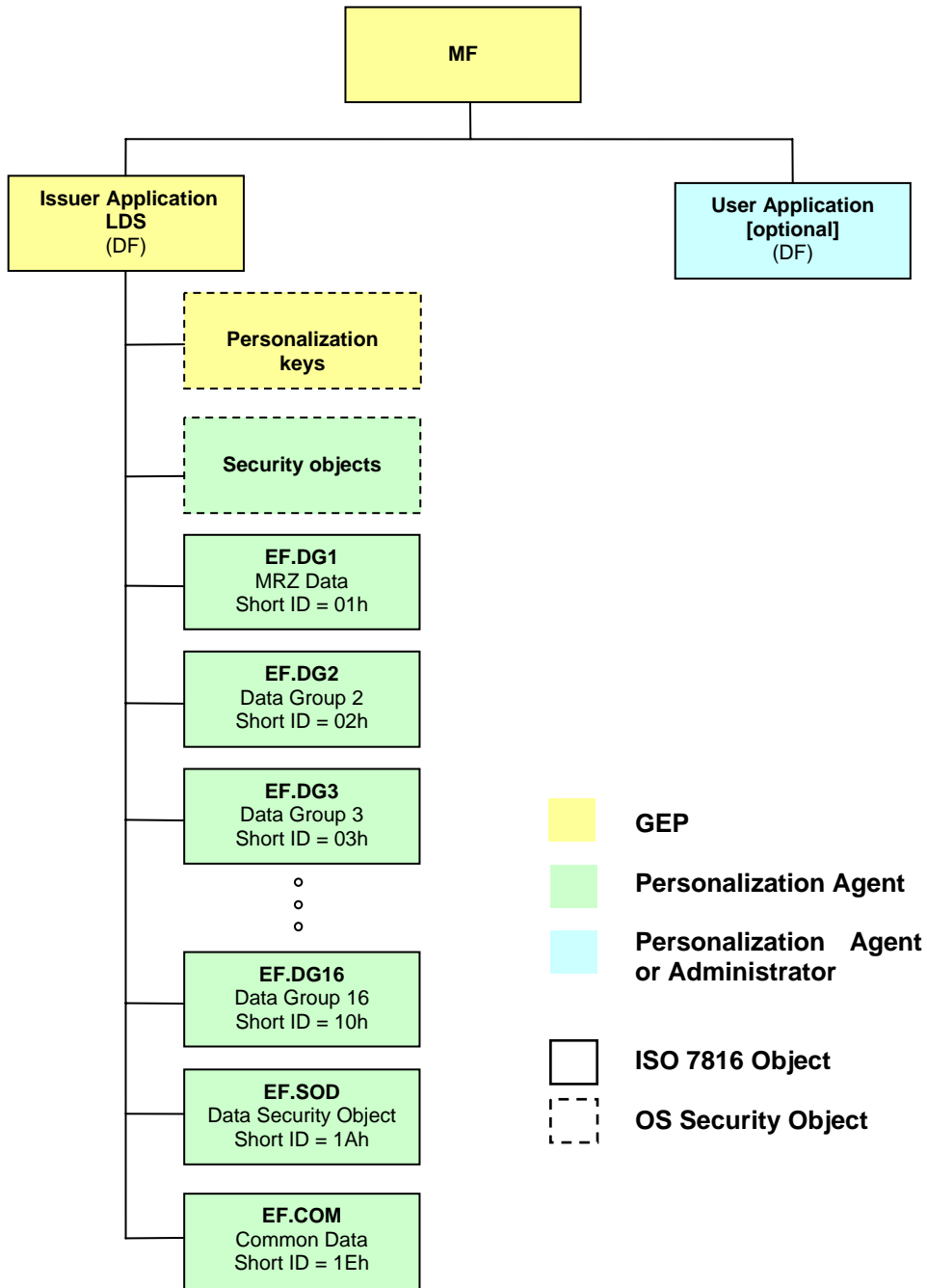


Figure2: Logical TOE

3.3 TOE 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 the context of this security target contains:

- Visual Inspection Zone (VIZ) containing biographical data and portrait of the holder,
- a separate data summary for visual and machine reading using Optical Character Recognition (OCR) functionality in the Machine Readable Zone (MRZ),
- Data Groups (DG) as specified by ICAO [R15] present in the LDS of the MRTD chip.

The authentication of the traveler is based on:

- the possession of a valid MRTD personalized for the traveler with the claimed identity as given on the biographical data page and
- biometrics using the reference data stored in the MRTD chip.

The issuing state or organization ensures the authenticity of the data of genuine MRTDs, while the receiving state trusts a genuine MRTD of an issuing state or organization.

For this security target the MRTD is viewed as unit of:

- 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:
 - the biographical data on the biographical data page of the passport book,
 - the printed data in the Machine-Readable Zone (MRZ),
 - the printed portrait
- the *logical MRTD* as data of the MRTD holder stored according to the Logical Data Structure 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:
 - the digital Machine Readable Zone Data (digital MRZ data, DG1),
 - the digitized portraits (DG2),
 - the optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both;
 - the other LDS DGs (DG5 to DG13, DG16)
 - the Document security object (SO_D),
 - security data objects required for product management.

The issuing state or organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The printed MRTD and the MRTD's chip are 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) [R13]. These security measures include the binding of the MRTD's chip to the passport book.

3.4 TOE Security Features

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 as well as the security features of the MRTD's chip.

ICAO [R16] defines the baseline required security methods Passive Authentication and the following optional advanced security methods:

- BAC,
- Active Authentication,
- Extended Access Control.

Passive Authentication and data encryption are performed completely and independently on the TOE by the TOE environment.

This security target addresses the protection of data integrity and confidentiality of the logical MRTD by the following means:

- in integrity by write-once access control enforced by logical and physical means,
- in confidentiality by the BAC Mechanism.

This security target does not address Active Authentication and Extended Access Control as optional security mechanisms.

The BAC mechanism is a security feature which shall be supported by the TOE but may be disabled by the issuing state or organization.

The inspection system:

- reads the printed data in the MRZ,
- authenticates itself by means of the keys derived from MRZ data.

The authentication of an inspection system is based on the use of random numbers. Random data is essential for cryptography as well as for physical security mechanisms. The Infineon chip is equipped with a true random generator based on physical probabilistic controlled effects. The random data are used from the Smartcard Embedded Software as well as from the security enforcing functions.

After successful authentication of the inspection system, the MRTD chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [R16], [R15].

The TOE provides also a set of administrative commands which may be used during the operational phase of the TOE life cycle.

3.5 TOE Life-cycle

Figure3 illustrates the five phases of the TOE life cycle states which are as follows:

1. development
2. manufacturing
3. personalization
4. operational use
5. terminated

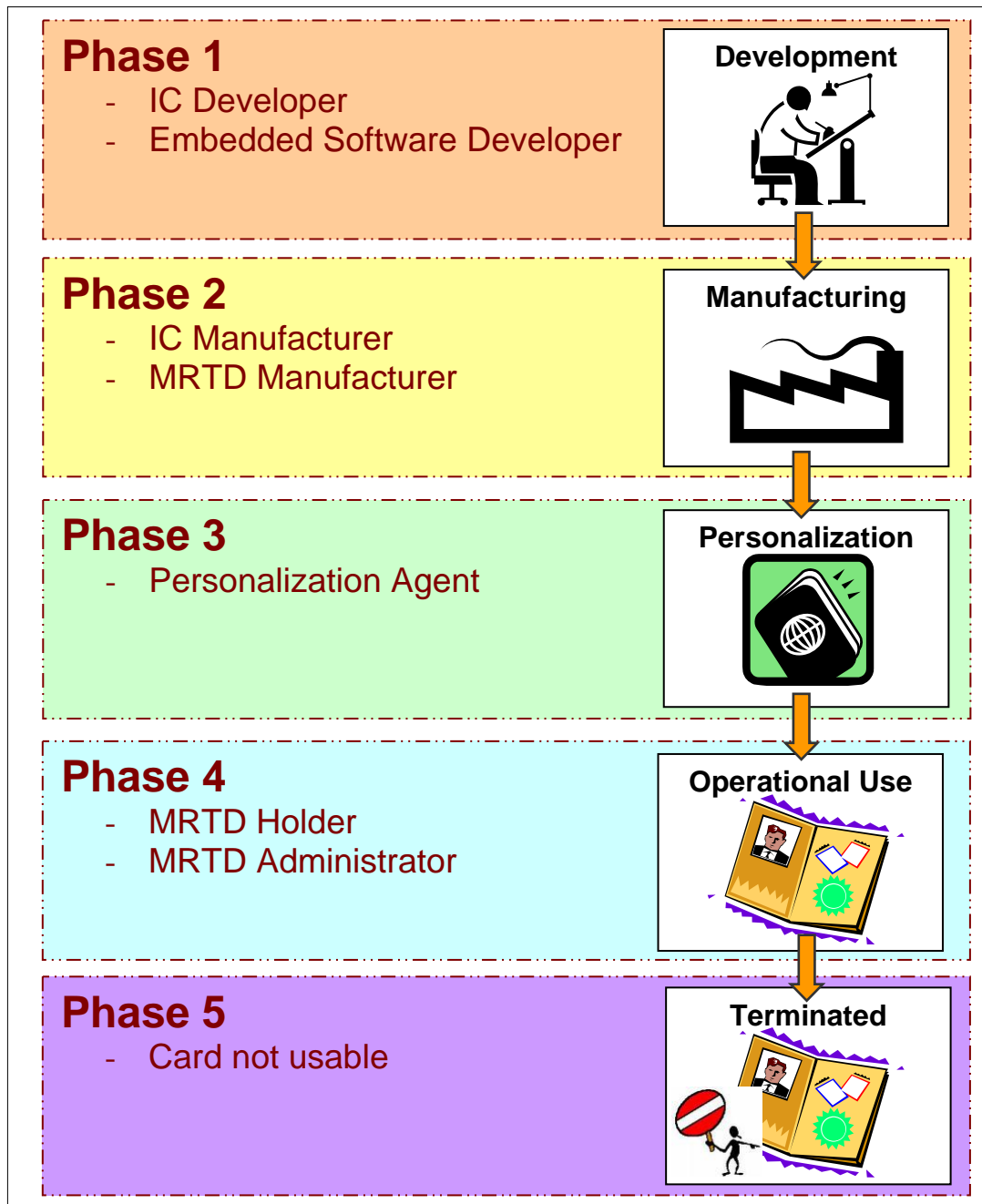


Figure3: TOE Life Cycle

3.5.1 Development

The TOE is developed in phase 1. The IC developer develops the IC, the IC dedicated software and the technical documentation associated with these TOE components. The firmware developer uses the IC's technical documentation (datasheet and relevant parts of the IC dedicated software) and develops the IC embedded software (operating system and MRTD LDS application) as well as the technical 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

non-volatile programmable memories, the MRTD application and the technical documentation is securely delivered to the MRTD manufacturer.

3.5.2 Manufacturing

In a first step of this phase the TOE IC is produced containing the MRTD's chip dedicated software and the parts of the MRTD's chip embedded software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip so as to track it as MRTD material during 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:

- adds the parts of the IC embedded software in the non-volatile programmable memories (for instance EEPROM) if necessary;
- creates the MRTD application;
- equips MRTD's chip with pre-personalization Data.

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

3.5.3 Personalization of the MRTD

The personalization of the MRTD includes:

- survey of the MRTD holder biographical data;
- enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data);
- printing of the VIZ data onto the physical MRTD;
- writing the TOE User Data and TOE Security Functions (TSF) Data into the LDS of the logical MRTD;
- writing the TSF Data into the logical MRTD and 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 (DG1);

- the digitized portrait (DG2);
- the Document security object (SO_D).

The signing of the SO_D by the Document Signer [R16] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate documentation specifying TOE use if necessary) is handed over to the MRTD holder for operational use.

3.5.4 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.

The MRTD Administrator authenticates itself by a BAC-like mechanism.

3.5.5 Terminated

In respect to the Protection Profile, in this Security Target we assume that in operational phase the successfully authenticated MRTD Administrator can deactivate the MRTD application and irreversibly change life cycle status to "terminated". In this case, the whole card will be unusable.

4 TOE Security Environment

4.1 Introduction

4.1.1 Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip and in addition the authenticity of the MRTD chip.

The logical MRTD data consists of the data groups (DG1 to DG13, DG16) and the SO_D according to LDS [R15]. These data are user data of the TOE. The data groups DG1 to DG13 and DG16 contain personal data of the MRTD holder. The SO_D is used by the inspection system for Passive Authentication of the logical MRTD.

An additional asset is the authenticity of the MRTD chip. The authenticity of the MRTD's chip personalized by the issuing state or organization for the MRTD's holder is used by the traveler to authenticate himself as possessing a genuine MRTD.

4.1.2 Subjects

This security target considers the following subjects:

- **Manufacturer:** The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.
- **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.
- **Personalization Agent:** The agent who is acting on the 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. signing the SO_D as defined in the LDS [R15].

- **Inspection system:** A technical system used by the border control officer of the receiving state (i) in examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
 - I. **The Primary Inspection System (PIS)**
 - contains a terminal for the contactless communication with the MRTD's chip and
 - does not implement the terminals part of the BAC Mechanism.The PIS can read the logical MRTD only if the BAC is disable.
 - II. **The Basic Inspection System (BIS)**
 - contains a terminal for the contactless communication with the MRTD's chip,
 - implements the terminals part of the BAC Mechanism,
 - is authorized to read the logical MRTD using BAC by optically reading the printed data in the MRZ or other parts of the passport book providing this information.
 - III. **The Extended Inspection System (EIS)**
 - implements the Active Authentication Mechanism;
 - supports the terminals part of the Extended Access Control Authentication Mechanism;
 - is authorized by the issuing state or organization to read the optional biometric reference data.
- **Terminal:** A terminal is any technical system communicating with the TOE through the contactless interface.
- **Attacker:** A threat agent trying:
 - I. to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data),
 - II. to read or to manipulate the logical MRTD without authorization, or
 - III. to forge a genuine MRTD.
- **MRTD Administrator:** This actor, acting on behalf of the Issuing State or Organization, deals with TOE's administration in the phase Operational Use. Adding data (not modification) and invalidation of the MRTD application are tasks of the MRTD Administrator.
- **Administration Terminal:** A terminal used by the MRTD Administrator to perform TOE administration in phase 4.
- **Personalization Terminal:** A terminal used by the Personalization Agent to perform TOE personalization and configuration in phase 3.

4.2 Assumptions

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

- **A.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 BAC Keys,
- iii. the Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and
- iv. the Document Signer Public Key Certificate (C_{DS}) 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 an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each Issuing State or Organization [R16]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by BAC. The Basic Inspection System implements the terminal part of the BAC and reads the logical MRTD being under BAC.

- **A.Holder_Behavior: Behavior of the MRTD holder**

The MRTD holder uses his/her passport in accordance to recommendations provided by the issuing state or organization which includes non-divulgence of the printed MRZ.

4.3 Threats

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

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

- **T.Chip_ID: Identification of MRTD's chip**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless

communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

- **T.Skimming: Skimming the logical MRTD**

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

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

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

Note that in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without help from the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

- **T.Forgery: Forgery of data on MRTD's chip**

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose 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 an other identity of the traveller. 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 MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MTRD'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 in an other contactless chip.

The TOE shall avert the threat as specified below.

- **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 User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

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

- **T.Information_Leakage: Information Leakage from MRTD's chip**

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

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the 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).

- **T.Phys_Tamper: Physical Tampering**

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) to 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 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.

- **T.Malfunction: Malfunction due to Environmental Stress**

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

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misuse of

administration function. To exploit this an attacker needs information about the functional operation.

4.4 Organizational Security Policies

The TOE shall comply to the following organization security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (refer to CC part 1, sec. 5.1 [R6]).

- **P.Manufact: Manufacturing of the MRTD's chip**

The IC Manufacturer and MRTD Manufacturer ensures the quality and the security of the manufacturing process while controlling the MRTD's material in Phase 2 Manufacturing. The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent's Keys.

- **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 authorized agents of the Issuing State or Organization only.

- **P.Personal_Data: Personal data protection policy**

- I. The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitised portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG13, 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 BAC to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document BAC keys as defined in [R16].

5 Security Objectives

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

5.1 TOE Security Objectives

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 groups DG1 to DG13, DG16, the Document security object according to LDS [R12] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG13, DG16 and the TSF data can be written only once and can not be changed after personalization. The Document security object can be updated by authorized MRTD Administrator if data in the data groups DG3 to DG13, DG16 are added in operational phase. Only the Personalization Agent shall be allowed to enable or to disable the TSF BAC.

- **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. If the TOE is configured for the use with Basic Inspection Terminals only, 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**

If the TOE is configured for the use with the BIS the TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG13, DG16 by granting read access to terminals successfully authenticated by (i) as the MRTD Administrator or (ii) as a BIS. The BIS shall authenticate itself by means of the BAC based on knowledge of the BAC Keys. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the BIS.

Moreover If the TOE is configured for the use with the PIS no protection in confidentiality of the logical MRTD is required.

- **OT.Identification: Identification and Authentication of the TOE**

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". In Phase 4 "Operational

Use" the TOEs shall identify themselves only to the successfully authenticated MRTD Administrator or BIS.

- **OT.Prot_Abuse_Func: Protection against Abuse of Functionality**

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order:

- to disclose critical User Data,
- to manipulate critical User Data of the Smartcard Embedded Software,
- to manipulate Soft-coded Smartcard Embedded Software,
- bypass, deactivate, change or explore security features or functions of the TOE.

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

The following TOE security objectives address the protection provided by the MRTD's chip independent on the TOE environment.

- **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,
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE.

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

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current),
- 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 has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

- **OT.Administration: Security of administrative commands in operational use**

The TOE must provide secure administrative commands to the MRTD Administrator in phase Operational Use. The TOE must prevent the use of these commands from unauthorized users. These commands are performed by means of Administration Terminals.

5.2 Environment Security Objectives

5.2.1 Development and Manufacturing Environment

- **OD.Assurance: Assurance Security Measures in Development and Manufacturing Environment**

The developer and manufacturer ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication keys. The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with low attack potential and against direct attacks with high attack potential against security function that uses probabilistic or permutational mechanisms.

- **OD.Material: Control over MRTD Material**

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialize, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

5.2.2 Operational Environment

Issuing State or Organization

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

- **OE.Personalization: Personalization of logical MRTD**

The Issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the Issuing State or Organization:

- establish the correct identity of the holder and create biographic data for the MRTD,
- 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),
- personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the SO_D).

The Personalization Agents enable or disable the BAC function of the TOE according to the decision of the Issuing State or Organization. If the BAC function is enabled, the Personalization Agents generate the Document BAC Keys and store them in the MRTD's chip.

- **OE.Pass_Auth_Sign: Authentication of logical MRTD by Signature**

The Issuing State or Organization must:

- generate a cryptographic secure Country Signing Key Pair,
- ensure the secrecy of the Country Signing Private Key (KPr_{CSCA}) and sign C_{DS}'s in a secure operational environment,
- distribute the C_{DS} to Receiving States and Organizations maintaining its authenticity and integrity.

Moreover the Issuing State or organization must:

- generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys (KPr_{DS}),
- sign Document Security Objects of genuine MRTD in a secure operational environment only,
- distribute the Certificate of the Document Signing Public Key to receiving States and organizations. The digital signature in the Document Security Object include all data in the data groups DG1 to DG16 if stored in the LDS.

- **OE.Administration: Administration of logical MRTD**

The Issuing State or Organization must ensure that in phase 4 "operational use" the MRTD Administrator performs administrative commands, like update and termination of the MRTD application, with the defined physical and logical security measures.

Receiving State or Organization

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

- **OE.Exam_MRTD: Examination of the MRTD passport book**

The inspection system of the Receiving State 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.

- **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 the SO_D 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 Signing Public Key maintaining their authenticity and availability in all inspection systems.

- **OE.Prot_Logical_MRTD: Protection of data of the logical MRTD**

The inspection system of the Receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The Receiving State examining the logical MRTD being under BAC will use inspection systems which implement the terminal part of the BAC and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.

MRTD Holder

Application note: the security objective of the TOE environment OE.Secure_Handling like defined in the PP [R4] is refined as follows:

- **OE.Secure_Handling: Secure handling of the MRTD by MRTD holder**

The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MRTD with disabled BAC) will prevent unauthorized communication of the MRTD's chip with terminals through the contactless interface. If the TOE is configured for the use with Basic Inspection Systems, the holder of a MRTD will prevent attempts to disclose the logical MRTD by following recommendations for the protection of the MRZ against unauthorized people.

6 IT Extended Components Definition

This ST uses components defined as extensions to CC part 2 [R7]. Some of these components are defined in [R3], other components are defined in the protection profile [R4].

6.1 Definition of the FAU_SAS Family

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined in the PP [R4]. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family “Audit data storage (FAU_SAS)” is specified in the following table.

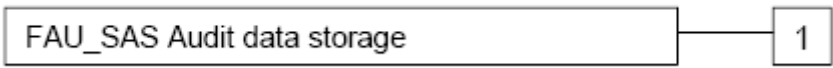
| FAU_SAS Audit data storage | |
|----------------------------|---|
| <i>Family behavior:</i> | This family defines functional requirements for the storage of audit data. |
| <i>Component leveling:</i> |  <pre> classDiagram class FAU_SAS_Audit_data_storage class 1 FAU_SAS_Audit_data_storage -- 1 </pre> |
| FAU_SAS.1 | Requires the TOE to provide the possibility to store audit data. |
| <i>Management</i> | There are no management activities foreseen. |
| <i>Audit</i> | There are no actions defined to be auditable. |
| FAU_SAS.1 | Audit storage |
| <i>Hierarchical to:</i> | No other components |
| 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. |
| <i>Dependencies:</i> | No Dependencies. |

Table2: FAU_SAS Family

6.2 Definition of the FCS_RND Family

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in the PP [R4]. 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 as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

The family “Generation of random numbers (FCS_RND)” is specified in the following table.


| FCS_RND Generation of random numbers | |
|--------------------------------------|---|
| <i>Family behavior:</i> | This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes. |
| <i>Component leveling:</i> |  |
| FCS_RND.1 | Generation of random numbers requires that random numbers meet a defined quality metric. |
| <i>Management:</i> | There are no management activities foreseen. |
| <i>Audit:</i> | There are no actions defined to be auditable. |
| FCS_RND.1 | Quality metric for random numbers |
| <i>Hierarchical to:</i> | No other components |
| FCS_RND.1.1 | The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric]. |
| <i>Dependencies:</i> | No Dependencies. |

Table3: FCS_RND Family

6.3 Definition of the FIA_API Family

To describe the IT security functional requirements of the TOE an additional family (FIA_API) of the Class FIA (Identification and authentication) is defined in the PP [R4]. This family describes the functional requirements for the proof of a the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

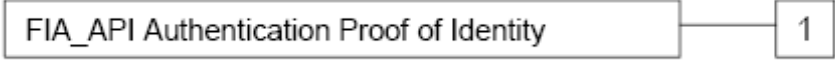
| FIA_API Authentication Proof of Identity | |
|--|---|
| <i>Family behavior:</i> | This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment. |
| <i>Component leveling:</i> |  |
| FIA_API.1 | Authentication Proof of Identity. |
| <i>Management:</i> | The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule]. |
| <i>Audit:</i> | There are no actions defined to be auditable. |
| FIA_API.1 | Authentication Proof of Identity |
| <i>Hierarchical to:</i> | No other components |
| FIA_API.1.1 | The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule]. |
| <i>Dependencies:</i> | No Dependencies. |

Table4: FIA_API Family

6.4 Definition of the FMT_LIM Family

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

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

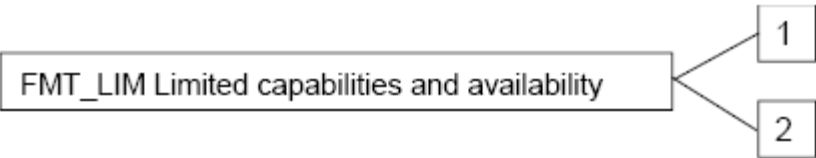
| FMT_LIM Limited capabilities and availability | |
|---|---|
| <i>Family behavior:</i> | This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner. |
| <i>Component leveling:</i> |  |
| 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. |
| <i>Management:</i> | There are no management activities foreseen. |
| <i>Audit:</i> | There are no actions defined to be auditable. |
| FMT_LIM.2 | Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle. |
| <i>Management:</i> | There are no management activities foreseen. |
| <i>Audit:</i> | There are no actions defined to be auditable. |

Table5: FMT_LIM Family

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

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

| FMT_LIM.1 | Limited capabilities |
|-------------------------|--|
| <i>Hierarchical to:</i> | No other components |
| 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]. |
| <i>Dependencies:</i> | FMT_LIM.2 Limited availability. |

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

| | |
|-------------------------|--|
| FMT_LIM.2 | Limited capabilities |
| <i>Hierarchical to:</i> | No other components |
| 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]. |
| <i>Dependencies:</i> | FMT_LIM.1 Limited capabilities. |

6.5 Definition of the FPT_EMSEC Family

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined in the PP [R4] to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD 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 [R7].

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

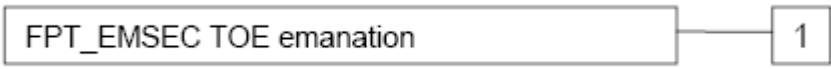
| FPT_EMSEC | |
|----------------------------|---|
| <i>Family behavior:</i> | This family defines requirements to mitigate intelligible emanations. |
| <i>Component leveling:</i> |  |
| FPT_EMSEC.1 | TOE emanation has two constituents: <ul style="list-style-type: none"> • FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data. • FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data. |
| <i>Management:</i> | There are no management activities foreseen. |
| <i>Audit:</i> | There are no actions defined to be auditable. |
| FPT_EMSEC.1 | TOE Emanation |
| <i>Hierarchical to:</i> | No other components |
| FPT_EMSEC.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_EMSEC.1.2 | The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data]. |
| <i>Dependencies:</i> | No dependencies. |

Table6: FPT_EMSEC Family

7 IT Security Requirements

7.1 Security Functional Requirements for the TOE

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

7.1.1 Class FAU Security Audit

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (CC part 2).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

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

Dependencies: No dependencies.

7.1.2 Class Cryptographic Support (FCS)

7.1.2.1 FCS_CKM.1

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (CC part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/BAC_MRTD Cryptographic key generation – Generation of Document BAC Keys by the TOE

Hierarchical to: No other components.

| | |
|--------------------------|---|
| FCS_CKM.1.1/ BAC_MRTD | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Keys Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [R16], Annex E. |
|--------------------------|---|

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1/PER_MRTD Cryptographic key generation – Generation of Personalization Keys by the TOE

Hierarchical to: No other components.

| | |
|--------------------------|---|
| FCS_CKM.1.1/ PER_MRTD | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <u>Personalization Keys Generation Algorithm</u> and specified cryptographic key sizes <u>112 bit</u> that meet following: <u>section 5.2</u> , <u>[R9]</u> |
|--------------------------|---|

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

7.1.2.2 FCS_CKM.4

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

FCS_CKM.4/MRTD Cryptographic key destruction - MRTD

Hierarchical to: No other components.

| | |
|-------------|---|
| FCS_CKM.4.1 | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method <u>physical deletion by overwriting the memory data with zeros</u> that meets the following: <u>none</u> . |
|-------------|---|

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

7.1.2.3 FCS_COP.1

The TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (CC part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/
SHA_MRTD

The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **none** that meet the following: **FIPS 180-2 [R11]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

Hierarchical to: No other components.

FCS_COP.1.1/
TDES_MRTD

The TSF shall **perform secure messaging – encryption and decryption** in accordance with a specified cryptographic algorithm **TDES in CBC mode** and cryptographic key sizes **112 bit** that meet the following: **FIPS 46-3 [R10] and Annex E of TR-PKI [R16]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/
MAC_MRTD

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) [R19]**.

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

FCS_CKM.1 Cryptographic key generation]
 FCS_CKM.4 Cryptographic key destruction
 FMT_MSA.2 Secure security attributes

The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (CC part 2 extended).

7.1.2.4 FCS_RND.1

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

| | |
|----------------------|--|
| FCS_RND.1.1/ MRTD | The TSF shall provide a mechanism to generate random numbers that meets functionality class P1-high of AIS31 [R1] . |
|----------------------|--|

Dependencies: No dependencies.

7.1.3 Class FIA Identification and Authentication

| Mechanism | SFR (TOE) | SFR (TOE Environment - Terminal) | Algorithm (Key Size)* |
|---|----------------------------------|----------------------------------|--|
| BAC | FIA_UAU.4/MRTD FIA_UAU.6/MRTD | FIA_UAU.4/BAC_T FIA_UAU.6/T | TDES (112 bits) Retail MAC (112 bits) |
| Symmetric Authentication Mechanism for Personalization Agents | FIA_UAU.4/MRTD | FIA_API.1/PT | TDES (112 bits) Retail MAC (112 bits) |
| Symmetric Authentication Mechanism for MRTD Administrator | FIA_UAU.4/MRTD | FIA_API.1/AT | TDES (112 bits) Retail MAC (112 bits) |

Table7: Authentication Mechanisms

7.1.3.1 FIA_AFL.1

The TOE shall meet the requirement “Authentication failures (FIA_AFL.1)” as specified below (CC part 2).

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

| | |
|-------------|---|
| FIA_AFL.1.1 | The TSF shall detect when [assignment: a positive integer number] unsuccessful authentication attempts occur related to [assignment: list of authentication events] . |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions] . |

Refinement: refer to Table8.

| Assignment: Number | Assignment: Authentication Events | Assignment: Actions |
|--------------------|--|--|
| 1 | Unsuccessful BAC authentication | User data and TSF data reading prevented |
| 1 | Unsuccessful MAC verification after BAC authentication | BAC session closed |
| 4 | Unsuccessful mutual authentication with Personalization Agent keys | Personalization Agent keys blocked |
| 4 | Unsuccessful mutual authentication with MRTD Administrator keys | MTRD Administrate keys blocked |

Table8: FIA_AFL.1 Refinement

Dependencies: FIA_UAU.1 Timing of authentication

7.1.3.2 FIA_UID.1

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (CC part 2).

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

| | |
|-------------|---|
| FIA_UID.1.1 | The TSF shall allow <ol style="list-style-type: none"> 1. <u>to read the Initialization Data in Phase 2,</u> 2. <u>to read the logical MRTD if the TOE is configured for use with PIS's in phase 4</u> 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. |

Dependencies: No dependencies.

7.1.3.3 FIA_UAU.1

The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (CC part 2).

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

| | |
|-------------|---|
| FIA_UAU.1.1 | The TSF shall allow <ol style="list-style-type: none">1. <u>to read the Initialization Data in Phase 2.</u>2. <u>to read the logical MRTD if the TOE is configured for use with PIS in phase 4</u> 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. |

Dependencies: FIA_UID.1 Timing of identification.

7.1.3.4 FIA_UAU.4

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (CC part 2).

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

Hierarchical to: No other components.

| | |
|------------------|---|
| FIA_UAU.4.1/MRTD | The TSF shall prevent reuse of authentication data related to <ol style="list-style-type: none">(1) <u>BAC Authentication Mechanism.</u>(2) <u>Authentication Mechanism based on TDES.</u> |
|------------------|---|

Dependencies: No dependencies.

7.1.3.5 FIA_UAU.5

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

FIA_UAU.5/MRTD Multiple authentication mechanisms

Hierarchical to: No other components.

| | |
|----------------------|---|
| FIA_UAU.5.1/ MRTD | The TSF shall provide (1) <u>BAC Authentication Mechanism</u> (2) <u>Symmetric Authentication Mechanism based on TDES</u> to support user authentication. |
| FIA_UAU.5.2/ MRTD | The TSF shall authenticate any user's claimed identity according to the <u>following rules:</u> (1) <u>the TOE accepts the authentication attempt as Personalization Agent by means of the Symmetric Authentication Mechanism with the Personalization Agent Keys (AK_{PA}).</u> (2) <u>the TOE accepts the authentication attempt as the BIS only by means of the BAC Authentication Mechanism with the Document Basic Access Keys.</u> (3) <u>the TOE accepts the authentication attempt as MRTD Administrator only by means of the Symmetric Authentication Mechanism with MRTD Administrator Keys (AK_{MA}).</u> |

Dependencies: No dependencies.

7.1.3.6 FIA_UAU.6

The TOE shall meet the requirement “Re-authenticating (FIA_UAU.6)” as specified below (CC part 2).

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

Hierarchical to: No other components.

| | |
|----------------------|--|
| FIA_UAU.6.1/ MRTD | The TSF shall re-authenticate the user under the conditions <u>each command sent to TOE after successful authentication of the terminal with BAC Authentication and Personalization Agent Authentication Mechanism.</u> |
|----------------------|--|

Dependencies: No dependencies.

7.1.4 Class FDP User Data Protection

7.1.4.1 FDP_ACC.1

The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below (CC part 2). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

FDP_ACC.1/PRIM Subset access control – Primary Access Control

Hierarchical to: No other components.

| | |
|----------------------|---|
| FDP_ACC.1.1/ PRIM | The TSF shall enforce the <u>Primary Access Control SFP</u> on <u>terminals gaining write, read and modification access to data groups DG1 to DG13, DG16 of the logical MRTD, EF.SOD, EF.COM and specific security data objects (keys and security environments).</u> |
|----------------------|---|

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1/BASIC Subset access control – BAC

Hierarchical to: No other components.

| | |
|-----------------------|--|
| FDP_ACC.1.1/ BASIC | The TSF shall enforce the <u>BAC SFP</u> on <u>terminals gaining write, read and modification access to data groups DG1 to DG13, DG16 of the logical MRTD, EF.SOD, EF.COM and specific security data objects (keys and security environments).</u> |
|-----------------------|--|

Dependencies: FDP_ACF.1 Security attribute based access control

7.1.4.2 FDP_ACF.1

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (CC part 2). The instantiations of FDP_ACC.1 address different SFP.

FDP_ACF.1/PRIM Security attribute based access control – Primary Access Control

Hierarchical to: No other components.

| | |
|--------------------------|---|
| <p>FDP_ACF.1.1/ PRIM</p> | <p>The TSF shall enforce the <u>Primary Access Control SFP</u> to objects based on the following:</p> <p>(1) <u>Subjects:</u></p> <ul style="list-style-type: none"> - <u>Personalization Agent,</u> - <u>MRTD Administrator,</u> - <u>Terminals.</u> <p>(2) <u>Objects:</u></p> <ul style="list-style-type: none"> - <u>data in the data groups DG1 to DG13, DG16 of the logical MRTD,</u> - <u>data in EF.COM,</u> - <u>data in EF.SO_D,</u> - <u>data in security data objects (keys and security environments).</u> <p>(3) <u>Security attributes:</u></p> <ul style="list-style-type: none"> - <u>configuration of the TOE according to FMT MOF.1,</u> - <u>authentication status of terminals.</u> |
| <p>FDP_ACF.1.2/ PRIM</p> | <p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>in the TOE configuration for use with PIS's:</u></p> <ol style="list-style-type: none"> 1. <u>the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D and specific security data objects (keys and security environments).</u> 2. <u>the successfully authenticated MRTD Administrator is allowed:</u> <ul style="list-style-type: none"> - <u>to add data to the data groups DG3 to DG13, DG16 of the logical MRTD,</u> - <u>to update EF.COM, EF.SO_D.</u> 3. <u>the Terminals are allowed to read the data of the groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D.</u> |
| <p>FDP_ACF.1.3/ PRIM</p> | <p>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none.</u></p> |
| <p>FDP_ACF.1.4/ PRIM</p> | <p>The TSF shall explicitly deny access of subjects to objects based on the rule: <u>the Terminals are not allowed to modify any of the data groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D and specific security data objects (keys and security environments).</u></p> |

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1/BASIC Security attribute based access control – BAC

Hierarchical to: No other components.

| | |
|---------------------------|---|
| <p>FDP_ACF.1.1/ BASIC</p> | <p>The TSF shall enforce the <u>BAC SFP</u> to objects based on the following:</p> <ol style="list-style-type: none"> 1. <u>Subjects</u> <ul style="list-style-type: none"> - <u>Personalization Agent</u> - <u>MRTD Administrator</u> - <u>BIS</u> - <u>Terminals</u> 2. <u>Objects</u> <ul style="list-style-type: none"> - <u>data in DGs DG1 to DG13, DG16 of the logical MRTD</u> - <u>data in EF.COM</u> - <u>data in EF.SO_D</u> - <u>data in OS security data objects (keys and security environment settings)</u> 3. <u>Security attributes</u> <ul style="list-style-type: none"> - <u>Configuration of the TOE according to FMT MOR.1</u> - <u>Authentication status of terminals</u> |
| <p>FDP_ACF.1.2/ BASIC</p> | <p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:</p> <ol style="list-style-type: none"> 1. <u>the successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D</u> 2. <u>the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D and specific security data objects (keys and security environment settings)</u> 3. <u>the successfully authenticated MRTD Administrator is allowed:</u> <ul style="list-style-type: none"> - <u>to read and to add data to the data groups DG3 to DG13, DG16 of the logical MRTD,</u> - <u>to read and to update EF.COM, EF.SO_D</u> |
| <p>FDP_ACF.1.3/ BASIC</p> | <p>The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none</u>.</p> |
| <p>FDP_ACF.1.4/ BASIC</p> | <p>The TSF shall explicitly deny access of subjects to objects based on the rule: <u>the Terminals are not allowed to modify any of the data groups DG1 to DG13, DG16 of the logical MRTD, EF.COM, EF.SO_D and specific security data objects (keys and security environments).</u></p> |

Dependencies: FDP_ACC.1 Subset access control
 FMT_MSA.3 Static attribute initialization

7.1.4.3 FDP_UCT.1

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

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

| | |
|----------------------|---|
| FDP_UCT.1.1/ MRTD | The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure. |
|----------------------|---|

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

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UIT.1)” as specified below (CC part 2).

7.1.4.4 FDP_UIT.1

FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

| | |
|----------------------|---|
| FDP_UIT.1.1/ MRTD | The TSF shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors . |
| FDP_UIT.1.2/ MRTD | The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred. |

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

7.1.5 Class FMT Security Management

The TOE shall meet the requirement “Management of functions in TSF (FMT_MOF.1)” as specified below (CC part 2).

FMT_MOF.1 Management of functions in TSF

Hierarchical to: No other components

| | |
|-------------|---|
| FMT_MOF.1.1 | The TSF shall restrict the ability to <u>enable and disable</u> the functions <u>TSF Basic Access Control</u> to <u>Personalization Agent</u> . |
|-------------|---|

Dependencies: No Dependencies

7.1.5.1 FMT_SMF.1

The TOE shall meet the requirement “Specification of Management Functions (FMT_SMF.1)” as specified below (CC part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

| | |
|-------------|--|
| FMT_SMF.1.1 | The TSF shall be capable of performing the following security management functions: <ol style="list-style-type: none">1. <u>Creation,</u>2. <u>Initialization,</u>3. <u>Personalization,</u>4. <u>Configuration,</u>5. <u>Administration.</u> |
|-------------|--|

Dependencies: No Dependencies

7.1.5.2 FMT_SMR.1

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below (CC part 2).

FMT_SMR.1 Security roles

Hierarchical to: No other components.

| | |
|-------------|--|
| FMT_SMR.1.1 | The TSF shall maintain the roles: <ol style="list-style-type: none">1. <u>Manufacturer</u>2. <u>Personalization Agent</u>3. <u>Primary Inspection System</u>4. <u>Basic Inspection System</u>5. <u>MRTD Administrator.</u> |
| FMT_SMR.1.2 | The TSF shall be able to associate users with roles. |

Hierarchical to: FIA_UID.1 Timing of identification.

7.1.5.3 FMT_LIM.1

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

| | |
|-------------|--|
| 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: <u>Deploying Test Features after TOE Delivery does not allow:</u> <ol style="list-style-type: none">1. <u>User Data to be disclosed or manipulated.</u>2. <u>TSF data to be disclosed or manipulated.</u>3. <u>software to be reconstructed and</u>4. <u>substantial information about construction of TSF to be gathered which may enable other attacks.</u> |
|-------------|--|

Dependencies: FMT_LIM.2 Limited availability.

7.1.5.4 FMT_LIM.2

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below (CC part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

| | |
|-------------|---|
| 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: <u>Deploying Test Features after TOE Delivery does not allow:</u> <ol style="list-style-type: none">1. <u>User Data to be disclosed or manipulated.</u>2. <u>TSF data to be disclosed or manipulated.</u>3. <u>software to be reconstructed and</u>4. <u>substantial information about construction of TSF to be gathered which may enable other attacks.</u> |
|-------------|---|

Dependencies: FMT_LIM.1 Limited capabilities.

The TOE shall meet the requirement “Management of TSF data (FMT_MTD.1)” as specified below (CC part 2). The iterations address different management functions and different TSF data.

7.1.5.5 FMT_MTD.1

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

Hierarchical to: No other components.

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

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

| | |
|-------------------------|--|
| FMT_MTD.1.1/ INI_DIS | The TSF shall restrict the ability to <u>disable read access for users</u> to the <u>Initialization Data and Pre-personalization Data</u> to the <u>Personalization Agent</u> . |
|-------------------------|--|

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1/INI_READ Management of TSF data – Reading of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

| | |
|--------------------------|--|
| FMT_MTD.1.1/ INI_READ | The TSF shall restrict the ability to read the <u>Initialization Data and the Pre-personalization Data (TOE identification data)</u> to the <u>Personalization Agent and the MRTD Administrator</u> . |
|--------------------------|--|

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

| | |
|---------------------------|--|
| FMT_MTD.1.1/ KEY_WRITE | The TSF shall restrict the ability to write the <u>Document Basic Access Keys and the MRTD Administrator Keys</u> to the <u>Personalization Agent</u> . |
|---------------------------|--|

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

| | |
|--------------------------|---|
| FMT_MTD.1.1/ KEY_READ | The TSF shall restrict the ability to read the <u>Document Basic Access Keys, the Personalization Agent Keys and the MRTD Administrator Keys</u> to none . |
|--------------------------|---|

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

7.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_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 SFR “Non-bypassability of the TSP (FPT_RVM.1)” and “TSF domain separation (FPT_SEP.1)” together with “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement “Subset information flow control (FPT_EMSEC.1)” as specified below (CC part 2 extended):

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

| | |
|---------------|--|
| FPT_EMSEC.1.1 | The TOE shall not emit <u>electromagnetic and current emissions</u> in excess of <u>intelligible threshold</u> enabling access to: <ol style="list-style-type: none">1. <u>Personalization Agent Authentication Keys,</u>2. <u>MRTD Administrator Authentication Keys,</u>3. <u>Document Basic Access Keys,</u> and: <ol style="list-style-type: none">1. <u>DG1 to DG13, DG16,</u>2. <u>EF.SO_D,</u>3. <u>EF.COM.</u> |
| FPT_EMSEC.1.2 | The TSF shall ensure <u>any unauthorized users</u> are unable to use the following interface <u>smart card circuit contacts</u> to gain access to: <ol style="list-style-type: none">1. <u>Personalization Agent Authentication Keys,</u>2. <u>MRTD Administrator Authentication Keys,</u>3. <u>Document Basic Access Keys,</u> and: <ol style="list-style-type: none">1. <u>DG1 to DG13, DG16,</u>2. <u>EF.SO_D,</u>3. <u>EF.COM.</u> |

Dependencies: No other components.

7.1.6.1 FPT_FLS

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

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

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

| | |
|-------------|--|
| FPT_FLS.1.1 | The TSF shall preserve a secure state when the following types of failures occur: <ol style="list-style-type: none">1. <u>exposure to operating conditions where therefore a malfunction could occur.</u>2. <u>failure detected by TSF according to FPT_TST.1.</u> |
|-------------|--|

Dependencies: ADV_SPM.1 Informal TOE security policy model

7.1.6.2 FPT_TST.1

The TOE shall meet the requirement “TSF testing (FPT_TST.1)” as specified below (CC part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components.

| | |
|-------------|---|
| FPT_TST.1.1 | The TSF shall run a suite of self tests <u>during initial start-up, before any use of TSF data</u> to demonstrate the correct operation of the TSF. |
| FPT_TST.1.2 | The TSF shall provide authorized users with the capability to verify the integrity of TSF data. |
| FPT_TST.1.3 | The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. |

Dependencies: FPT_AMT.1 Abstract machine testing.

7.1.6.3 FPT_PHP.3

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

| | |
|-------------|---|
| FPT_PHP.3.1 | The TSF shall resist <u>physical manipulation and physical probing</u> to the <u>TSF</u> by responding automatically such that the TSP is not violated. |
|-------------|---|

Dependencies: No dependencies.

7.1.6.4 FPT_RVM

The following security functional requirements protect the TSF against bypassing and support the separation of TOE parts.

The TOE shall meet the requirement “Non-bypassability of the TSP (FPT_RVM.1)” as specified below (CC part 2).

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

| | |
|-------------|--|
| FPT_RVM.1.1 | The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. |
|-------------|--|

Dependencies: No dependencies.

7.1.6.5 FPT_SEP

The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (CC part 2).

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

| | |
|-------------|---|
| FPT_SEP.1.1 | The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by un-trusted subjects. |
| FPT_SEP.1.2 | The TSF shall enforce separation between the security domains of subjects in the TSC. |

Dependencies: No dependencies.

7.2 Security Assurance Requirements for the TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV_IMP.2 and ALC_DVS.2.

The minimum strength of function is SOF-high.

This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

7.3 Security Requirements for the IT environment

This section describes the security functional requirements for the IT environment using the CC part 2 components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in *italic/bold*.

7.3.1 Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the CSCA Keys and the Document Signing Keys to support the signing of the User Data (DG1 to DG16) by means of the Document Security Object. TR-PKI [R15] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the Issuing State or Organization shall meet the requirement "Basic data authentication (FDP_DAU.1)" as specified below (CC part 2).

FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to: No other components.

| | |
|------------------|--|
| FDP_DAU.1/ DS | The Document Signer shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (DG1 to DG16) and the Document Security Object . |
|------------------|--|

| | |
|--------------------|--|
| FDP_DAU.1.2/ DS | The Document Signer shall provide Inspection Systems of Receiving States or Organization with the ability to verify evidence of the validity of the indicated information. |
|--------------------|--|

Dependencies: No dependencies

7.3.2 Personalization Terminals

The Personalization Terminal (PT) shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (CC part 2).

FCS_CKM.1/PT Cryptographic key generation – Generation of Personalization Keys by the Personalization Terminal

Hierarchical to: No other components.

| | |
|----------------|--|
| FCS_CKM.1.1/PT | The Personalization Terminal shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Personalization Keys Generation Algorithm and specified cryptographic key sizes 112 bit that meet following: sections 4.1, 5.2 [R9] . |
|----------------|--|

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FDP_ITC.2 Import of user data with security attributes, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4/PT Cryptographic key destruction - PT

Hierarchical to: No other components.

| | |
|----------------|--|
| FCS_CKM.4.1/PT | The Personalization Terminal shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method secure erase of the keys value that meets the following: none . |
|----------------|--|

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

FCS_COP.1/ENC_PT Cryptographic operation – Secure Messaging Encryption / Decryption by the Personalization Terminal

Hierarchical to: No other components.

| | |
|------------------------|--|
| FCS_COP.1.1/ ENC_PT | The <i>Personalization Terminal</i> shall perform <u>secure messaging – encryption and decryption</u> in accordance with a specified cryptographic algorithm <u>TDES in CBC mode</u> and cryptographic key sizes <u>112 bits</u> that meet the following: <u>FIPS 46-3 [R10], ISO 11568-2 [R20] and ISO 9797-1 (padding mode 2) [R19]</u> . |
|------------------------|--|

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_PT Cryptographic operation – Secure messaging Message Authentication Code by the Personalization Terminal

Hierarchical to: No other components.

| | |
|------------------------|---|
| FCS_COP.1.1/ MAC_PT | The <i>Personalization Terminal</i> shall perform <u>secure messaging – message authentication code</u> in accordance with a specified cryptographic algorithm <u>Retail-MAC</u> and cryptographic key sizes <u>112 bits</u> that meet the following: <u>FIPS 46-3 [R10] and ISO 9797-1 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2) [R19]</u> . |
|------------------------|---|

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

The PT shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (CC part 2 extended).

FCS_RND.1/PT Quality metric for random numbers - Personalization Terminal

Hierarchical to: No other components.

| | |
|----------------|--|
| FCS_RND.1.1/PT | The <i>PT</i> shall provide a mechanism to generate random numbers that meets <u>functionality class P1-high of AIS31 [R1]</u> . |
|----------------|--|

Dependencies: No dependencies.

The PT shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (CC part 2).

FIA_UAU.4/PT Single-use authentication mechanisms – Personalization Terminal

Hierarchical to: No other components.

| | |
|----------------|---|
| FIA_UAU.4.1/PT | The <i>Personalization Terminal</i> shall prevent reuse of authentication data related to PA Authentication Mechanism . |
|----------------|---|

Dependencies: No dependencies.

The PT shall meet the requirement “Re-authentication (FIA_UAU.6)” as specified below (CC part 2).

FIA_UAU.6/PT Re-authentication - Personalization Terminal

Hierarchical to: No other components.

| | |
|----------------|---|
| FIA_UAU.6.1/PT | The <i>Personalization Terminal</i> shall re-authenticate the user under the conditions <u>each command sent to TOE after successful authentication of the terminal with Personalization Agent Authentication Mechanism</u> . |
|----------------|---|

Dependencies: No dependencies.

The PT shall meet the requirement “Personalization data exchange confidentiality (FDP_UCT.1)” as specified below (CC part 2).

FDP_UCT.1/PT Personalization data exchange confidentiality – Personalization Terminal

Hierarchical to: No other components.

| | |
|----------------|--|
| FDP_UCT.1.1/PT | The <i>Personalization Terminal</i> shall enforce the <u>PT part of BAC SFP</u> to be able to <u>transmit and receive</u> objects in a manner protected from unauthorized disclosure. |
|----------------|--|

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

The Personalization Terminal shall meet the requirement “Personalization data exchange confidentiality (FDP_UIT.1)” as specified below (CC part 2).

FDP_UIT.1/PT Data exchange integrity - PT

Hierarchical to: No other components.

| | |
|----------------|---|
| FDP_UIT.1.1/PT | The <i>Personalization Terminal</i> shall enforce the <u>PT part of Basic Access Control SFP</u> to be able to <u>transmit and receive</u> user data in a manner protected from <u>modification, deletion, insertion and replay</u> errors. |
| FDP_UIT.1.2/PT | The <i>Personalization Terminal</i> shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> has occurred. |

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

The Personalization Terminal shall meet the requirement “Authentication Prove of Identity (FIA_API)” as specified below (CC part 2 extended).

FIA_API.1/SYM_PT Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Keys

Hierarchical to: No other components.

| | |
|------------------------|--|
| FIA_API.1.1/ SYM_PT | The <i>Personalization Terminal</i> shall provide a <u>Authentication Mechanism based on TDES</u> to prove the identity of the <u>Personalization Agent</u> . |
|------------------------|--|

Dependencies: No dependencies.

7.3.3 Administration Terminals

The Administration Terminal shall meet the requirement “Authentication Prove of Identity (FIA_API)” as specified below (CC part 2 extended).

FIA_API.1/SYM_AT Authentication Proof of Identity - Administration Terminal Authentication with Symmetric Key

Hierarchical to: No other components.

| | |
|------------------------|---|
| FIA_API.1.1/ SYM_PT | The Administration Terminal shall provide a Authentication Mechanism based on TDES to prove the identity of the MRTD Administrator . |
|------------------------|---|

Dependencies: No dependencies.

7.3.4 Basic Inspection Systems

This section describes common security functional requirements to the Basic Inspection Systems and the MRTD Administration Terminal (phase 4). All are called “Basic Terminals” (BT) in this section.

The Basic Terminal (BT) shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (CC part 2).

FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document BAC Keys by the Basic Terminal

Hierarchical to: No other components.

| | |
|------------------------|--|
| FCS_CKM.1.1/ BAC_BT | The Basic Terminal shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Keys Derivation Algorithm and specified cryptographic key sizes 112 bit that meet following: [R16], Annex E . |
|------------------------|--|

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FDP_ITC.2 Import of user data with security attributes, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4/BT Cryptographic key destruction - BT

Hierarchical to: No other components.

| | |
|----------------|--|
| FCS_CKM.4.1/BT | The Basic Terminal shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method secure erase of the keys value that meets the following: none . |
|----------------|--|

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

FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes.

The BT shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (CC part 2). The iterations are caused by different cryptographic algorithms to be implemented by the BT.

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

Hierarchical to: No other components.

| | |
|------------------------|--|
| FCS_COP.1.1/ SHA_BT | The Basic Terminal shall perform hashing in accordance with a specified cryptographic algorithms SHA-1 and cryptographic key sizes none that meet the following: FIPS 180-2 2 [R11] . |
|------------------------|--|

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to: No other components.

| | |
|------------------------|---|
| FCS_COP.1.1/ ENC_BT | The Basic Terminal shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm TDES in CBC mode and cryptographic key sizes 112 bits that meet the following: FIPS 46-3 [R10], ISO 11568-2 [R20] and ISO 9797-1 (padding mode 2) [R19] . |
|------------------------|---|

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

Hierarchical to: No other components.

| | |
|------------------------|--|
| FCS_COP.1.1/ MAC_BT | The Basic Terminal shall perform <u>secure messaging – message authentication code</u> in accordance with a specified cryptographic algorithm <u>Retail-MAC</u> and cryptographic key sizes <u>112 bits</u> that meet the following: <u>FIPS 46-3 [R10] and ISO 9797-1 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2) [R19]</u> . |
|------------------------|--|

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

The BT shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (CC part 2 extended).

FCS_RND.1/BT Quality metric for random numbers - Basic Terminal

Hierarchical to: No other components.

| | |
|----------------|--|
| FCS_RND.1.1/BT | The BT shall provide a mechanism to generate random numbers that meets <u>functionality class P1-high of AIS31 [R1]</u> . |
|----------------|--|

Dependencies: No dependencies.

The BT shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (CC part 2).

FIA_UAU.4/BT Single-use authentication mechanisms – Basic Terminal

Hierarchical to: No other components.

| | |
|----------------|---|
| FIA_UAU.4.1/BT | The BT shall prevent reuse of authentication data related to <u>BAC Authentication Mechanism</u> . |
|----------------|---|

Dependencies: No dependencies.

The BT shall meet the requirement “Re-authentication (FIA_UAU.6)” as specified below (CC part 2).

FIA_UAU.6/BT Re-authentication - Basic Terminal

Hierarchical to: No other components.

| | |
|----------------|--|
| FIA_UAU.6.1/BT | The Basic Terminal shall re-authenticate the user under the conditions <u>each command sent to TOE after successful authentication of the terminal with BAC Authentication Mechanism.</u> |
|----------------|--|

Dependencies: No dependencies.

The BT shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (CC part 2).

FDP_UCT.1/BT Basic data exchange confidentiality – BT

Hierarchical to: No other components.

| | |
|----------------|---|
| FDP_UCT.1.1/BT | The Basic Terminal shall enforce the <u>BT part of BAC SFP</u> to be able to <u>transmit and receive</u> objects in a manner protected from unauthorized disclosure. |
|----------------|---|

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

The Basic Terminal shall meet the requirement “Basic data exchange confidentiality (FDP_UIT.1)” as specified below (CC part 2).

FDP_UIT.1/BT Data exchange integrity - BT

Hierarchical to: No other components.

| | |
|----------------|---|
| FDP_UIT.1.1/BT | The Basic Terminal shall enforce the <u>BT part of Basic Access Control SFP</u> to be able to <u>transmit and receive</u> user data in a manner protected from <u>modification, deletion, insertion and replay</u> errors. |
| FDP_UIT.1.2/BT | The Basic Terminal shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> has occurred. |

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

8 TOE Summary Specification

8.1 TOE Security Functions

8.1.1 SF1

SF1: Agents Identification and Authentication

The Basic Access Control (for MRTD Holder authentication) and BAC-like mechanisms (for MRTD Administrator authentication) use a mutual authentication mechanism based on a three pass challenge-response protocol. The challenge is the random number sent from one party to the other. This random number will be enciphered with the secret symmetric key by the receiver and then will be verified by the sender. SF1 manages the session keys exchanged between the terminal and the TOE and provides the means to identify and authenticate the users in a secure way. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and Annex E of TR-PKI), while the message authentication code is according with Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). These authentication keys are derived by the SHA-1 algorithm (FIPS 180-2) like described in Annex E of ICAO TR-PKI.

Also the Personalization Agent authenticates itself by means of a mutual authentication mechanism.

The claimed strength of this function is high.

8.1.2 SF2

SF2: Data exchange with Secure Messaging

This function concerns the creation and the management of a secure communication channel for the sensitive data exchange between the TOE and the Inspection System. On this channel the data will be encrypted and authenticated with session keys (data TDES-encryption and MAC computation) such that the TOE is able to verify the integrity and authenticity of received data. The algorithm used for encryption/decryption is a Triple-DES in CBC mode with key sizes 112 bits (FIPS 46-3 and Annex E of TR-PKI), while the message authentication code is according with Retail MAC algorithm and cryptographic key sizes 112 bit (ISO 9797 - MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2). The session keys are calculated during the authentication phase.

The claimed strength of this function is high.

8.1.3 SF3

SF3: Access Control of stored Data Objects

SF3 enforces the Security Policies as required in FDP_ACF.1, i.e. controls the reading and writing access in different phases of the production and during operational use.

This function ensures that the assets (user data and TSF data) can only be accessed as defined by the access right written during the personalization process and allows the access to the TOE identification data in Personalization phase and to the successfully authenticated MRTD Administrator.

This function has no SOF-claim.

8.1.4 SF4

SF4: Life cycle management

This function ensures that the TOE life cycle status is set in irreversible way between the different phases following: manufacturing, personalization, operational use and terminated. When the MRTD application is invalidated by the MRTD Administrator and the TOE transits in terminated status, the data contained in MRTD application are no more available.

This function has no SOF-claim.

8.1.5 SF5

SF5: software integrity check of TOE's assets

The TOE doesn't allow to analyze, debug or modify TOE's software during the operational use.

Integrity checks will be executed before any use of TSF data.

This SF warns the entity connected upon detection of an integrity error of the stored sensitive data and preserves a secure state when failure is detected by TSF.

This function has no SOF-claim.

8.1.6 SF6

SF6: Security functions provided by the hardware

The Infineon chip provides a functionalities set used by the OS.

- Correct function of the chip is only given in specified range of parameters. To prevent an attack exploiting that circumstance, it checks if this specified range is left.

- The Infineon chip guarantees the separation between the security enforcing hardware functions and the user software.
- Several mechanisms protect the chip against snooping the design or user data during operation and even it is out of operation (power down).
- The readout of data can be controlled with the use of encryption. An attacker can not use the data obtained by espionage due to their encryption. The memory contents of the chip are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. Parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA. The current consumption is independent of the processed data. The information leakage is kept low with special design measures.
- The Infineon chip is equipped with a true random generator based on physical probabilistic controlled effects. It fulfil the requirements from the functionality class P1-high of [AIS31].
- The TSF hardware has a hardware controlled self test which can be started from the Smartcard Embedded Software. Any attempt to modify the sensor devices will be detected from the test.
- The entire surface of the chip is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contact.
- The (Memory Management Unit) MMU in the chip gives the Smartcard Embedded Software the possibility to define different access rights for memory areas and components.
- The chip is equipped with several hardware accelerators to support the standard cryptographic operations. The DDES (dual key DES) accelerator supports the Data Encryption Standard, DES, in ECB mode. This module is optimized for single DES and dual-key triple DES algorithm and works in high performance mode (HPM) or single step mode (SSM). Other modes like cipher block chaining (CBC), cipher feedback mode (CFB) or output feedback mode (OFB) have to be programmed by means of software, making use of the basic DES functions provided by the DDES accelerator. The ACE (Advanced Crypto Engine) is an arithmetic coprocessor dedicated to extremely fast modular and non-modular multiplication of very long integers. It allows to perform RSA 512 to 1024 bits and DSA 512 and 1024 bits.

This security function already has been evaluated and certified being already certified the chip [R2].

This SF has high SOF-claim.

8.2 SOF claim for TSF

For TSF described in this security target SOF-high is claimed. SF1 function manages identification and authentication based on mutual authentication while SF2 enforces data exchange with secure messaging. For these functions, the random number generator for the session keys and the encryption algorithms ensure resistance against direct attacks based on probabilistic or permutational mechanisms. In addition, the verification of the authentication PIN of the MRTD Manufacturer and of the authentication keys of the Personalization Agent and MRTD Administrator is enforced by a retry counter.

8.3 Assurance Measures

The documentation is produced in compliance with CC. The following documents provide the necessary information to fulfill the assurance requirements as defined in EAL4+ in this security target.

| Security Assurance Requirements | Documents |
|---------------------------------|--|
| ACM_AUT.1, ACM_CAP.4, ACM_SCP.2 | Configuration Management Plan, Configuration list, Acceptance plan |
| ADO_DEL.2, | Delivery documentation |
| ADV_FSP.2 | Functional Specification |
| ADV_HLD.2 | High Level Design |
| ADV_IMP.2 | Implementation representation |
| ADV_LLD.1 | Low Level Design |
| ADV_RCR.1 | Correspondence analysis |
| ADV_SPM.1 | TOE security policy model |
| AGD_ADM.1, ADO_IGS.1 | e-Passport Administrator Guidance |
| AGD_USR.1 | e-Passport User Guidance |
| ALC_DVS.2 | Development security documentation |
| ALC_LCD.1 | Life-cycle model documentation |
| ALC_TAT.1 | Development tools documentation |
| ATE_COV.2 | Test documentation |
| ATE_DPT.1 | High-level design test documentation |
| ATE_FUN.1 | Functional testing documentation |
| AVA_MSU.2 | Misuse analysis of the guidance |
| AVA_SOF.1 | Strength analysis of the TSF |
| AVA_VLA.2 | Vulnerability analysis |

Table9: Assurance Requirements documentation

9 Protection Profile Claims

The security target for the TOE claims conformance with the PP “*Machine Readable Travel Document with ICAO Application, BAC*“ BSI-PP-0017 [R4].

In respect to the PP, in the list of LDS DGs DG14 and DG15 are not present because this security target doesn't address Extended Access Control and Active Authentication.

Following subjects are added to the PP:

- MRTD Administrator,
- Administration Terminal.

The refinements and tailoring operated on the PP are:

- MRTD administrator is a new actor introduced in phase Operational Use for the management of the TOE.
- Administration Terminal provides administration functionalities.
- Threat T.Abuse-Func comprises the abuse of administration commands.

10 Rationale

10.1 Security Objectives Rationale

Table10 provides an overview for security objectives coverage.

| | OT.AC_Pers | OT.Data_Int | OT.Data_Conf | OT.Identification | OT.Prot_Abuse-Func | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OT.Administration | OD.Assurance | OD.Material | OE.Personalization | OE.Pass_Auth_Sign | OE.Administration | OE.Exam_MRTD | OE.Pass_Auth_Verif | OE.Prot_Logical_MRTD | OE.Secure_Handling |
|-----------------------|------------|-------------|--------------|-------------------|--------------------|------------------|---------------------|---------------------|-------------------|--------------|-------------|--------------------|-------------------|-------------------|--------------|--------------------|----------------------|--------------------|
| T.Chip-ID | | | | x | | | | | | | | | | | | | | x |
| T.Skimming | | | x | x | | | | | | | | | | | | | | x |
| T.Eavesdropping | | | x | x | | | | | | | | | | | | | | |
| T.Forgery | x | x | | | | | x | | | | | | x | | x | x | | |
| T.Abuse-Func | | | | | x | | | | x | x | x | x | | x | | | | |
| T.Information-Leakage | | | | | | x | | | | | | | | | | | | |
| T.Phys-Tamper | | | | | | | x | | | | | | | | | | | |
| T.Malfunction | | | | | | | | x | | | | | | x | | | | |
| P.Manufact | | | | | | | | | | x | x | | | | | | | |
| P.Personalization | x | | | | | | | | | x | | x | | | | | | |
| P.Personal_Data | | x | x | | | | | | | | | | | | | | | |
| A.Pers_Agent | | | | | | | | | | | | x | | | | | | |
| A.Insp_Sys | | | | | | | | | | | | | | | x | | x | |
| A.Holder_Behav | | | | | | | | | | | | | | | | | | x |

Table10: Security Objectives Rationale

The OSP **P.Manufact** “Manufacturing of the MRTD’s chip” requires the quality and integrity of the manufacturing process and control the MRTD’s material in the Phase 2 Manufacturing including unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data. The security objective for the TOE environment **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment” address these obligations of the IC Manufacturer and MRTD Manufacturer.

The OSP **P.Personalization** “Personalization of the MRTD by Issuing State or Organization only” 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 Authentication keys according to **OD.Assurance** “Assurance Security Measures in Development and Manufacturing Environment”. The security objective **OT.AC_Pers** limits the management of TSF data to the Personalization Agent.

The OSP **P.Personal_Data** “Personal data protection policy” requires the TOE (i) to support the protection of the confidentiality of the logical MRTD by means of the BAC 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” which describes the unconditional protection of the integrity of the stored data and the configurable integrity protection during the transmission. The security objective **OT.Data_Conf** “Confidentiality of personal data” describes the protection of the confidentiality as configured by the Personalization Agent acting in charge of the Issuing State or Organization.

The threat **T.Chip_ID** “Identification of MRTD’s chip” addresses the trace of the MRTD movement by identifying remotely the MRTD’s chip through the contactless communication interface. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered as described by the security objective **OT.Identification** by BAC. This threat shall be adverted also by the TOE environment as described by **OE.Secure_Handling** redefined in this security target.

The threat **T.Skimming** “Skimming digital MRZ data or the digital portrait” and **T.Eavesdropping** “Eavesdropping to the communication between TOE and inspection system” address the reading of the logical MRTD through the contactless interface or listening the communication between the MRTD’s chip and a terminal. In case of TOE configuration for use with Basic Inspection Terminals only this threat is countered by the security objective **OT.Identification** through BAC. The threat T.Skimming shall be adverted also by the TOE environment according to **OE.Secure_Handling** “Secure handling of the MRTD by MRTD holder” and the threat T.Eavesdropping shall be adverted by **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD”.

The threat **T.Forgery** “Forgery of data on MRTD’s chip” address 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 an additional 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".

The threat **T.Abuse-Func** "Abuse of Functionality" 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. The security objectives for the TOE environment **OD.Material** "Control over MRTD Material" ensures the control of the MRTD material. The security objective for the TOE environment **OD.Assurance** "Assurance Security Measures in Development and Manufacturing Environment" and **OE.Personalization** "Personalization of logical MRTD" ensure 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.

The security objectives **OT.Administration** and **OE.Administration** prevent misuse or abuse of administrative commands during the Operational Use.

The threats **T.Information_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats are addressed by the directly related security objectives **OT.Prot_Inf_Leak** "Protection against Information Leakage", **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot_Malfunction** "Protection against Malfunctions". Moreover, the security objective **OE.Administration** prevent the misuse of the administration functions by means of defined physical and logical security measures, covering the threat T.Malfunction.

The assumption **A.Pers_Agent** "Personalization of the MRTD's chip" 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 and the enabling of security features of the TOE according to the decision of the Issuing State or Organization concerning the BAC.

The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book". If the Issuing State of Organization decides to protect confidentiality of the logical MRTD then the security objective for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data of the logical MRTD" require the Basic Inspection System to implement the BAC and to protect the logical MRTD data during the transmission and the internal handling. If the Issuing State of Organization decides to configure the TOE for use with Primary Inspection Systems then no protection of the logical MRTD data is required by the inspection system.

The assumption **A.Holder_Behav** "Behaviour of the MRTD holder" addresses the passport use on the part of MRTD holder and is covered by the security objective **OE.Secure_Handling** as redefined in this security target.

10.2 Security Requirements Rationale

10.2.1 Security Objectives for the TOE

Table11 provides an overview for security functional requirements coverage.

| | OT.AC_Pers | OT.Data_Int | OT.Data_Conf | OT.Identification | OT.Prot_Inf_Leak | OT.Prot_Phys-Tamper | OT.Prot_Malfunction | OT.Prot_Abuse-Func | OT.Administration |
|---------------------|------------|-------------|--------------|-------------------|------------------|---------------------|---------------------|--------------------|-------------------|
| FAU_SAS.1 | | | | x | | | | | |
| FCS_CKM.1/BAC_MRTD | (x) | x | (x) | | | | | | |
| FCS_CKM.1/PER_MRTD | x | x | | | | | | | |
| FCS_CKM.4 | (x) | | x | | | | | | x |
| FCS_COP.1/SHA_MRTD | x | x | (x) | | | | | | |
| FCS_COP.1/TDES_MRTD | x | x | x | | | | | | |
| FCS_COP.1/MAC_MRTD | x | x | x | | | | | | |
| FCS_RND.1/MRTD | (x) | x | x | | | | | | |
| FIA_AFL.1 | x | | x | | | | | | x |
| FIA_UID.1 | | | x | x | | | | | x |
| FIA_UAU.1 | | | x | | | | | | x |
| FIA_UAU.4/MRTD | x | x | x | | | | | | x |
| FIA_UAU.5/MRTD | x | x | x | | | | | | x |
| FIA_UAU.6/MRTD | x | x | x | | | | | | |
| FDP_ACC.1/PRIM | x | x | | | | | | | x |
| FDP_ACF.1/PRIM | x | x | | | | | | | x |
| FDP_ACC.1/BASIC | x | x | x | | | | | | x |
| FDP_ACF.1/BASIC | x | x | x | | | | | | x |
| FDP_UCT.1/MRTD | x | x | x | | | | | | |
| FDP_UIT.1/MRTD | x | x | x | | | | | | |
| FMT_MOF.1 | x | x | x | | | | | | x |
| FMT_SMF.1 | x | x | x | | | | | | x |
| FMT_SMR.1 | x | x | x | | | | | | |
| FMT_LIM.1 | | | | | | | | x | |
| FMT_LIM.2 | | | | | | | | x | |
| FMT_MTD.1/INI_ENA | | | | x | | | | | |
| FMT_MTD.1/INI_DIS | | | | x | | | | | x |
| FMT_MTD.1/INI_READ | | | | x | | | | | x |
| FMT_MTD.1/KEY_WRITE | x | x | x | | | | | | |
| FMT_MTD.1/KEY_READ | x | x | x | | | | | | x |
| FPT_EMSEC.1 | x | | | | x | | | | x |
| FPT_TST.1 | | | | | x | | x | | |
| FPT_RVM.1 | | | | | | | | x | x |
| FPT_FLS.1 | x | | | | x | | x | | |
| FPT_PHP.3 | x | | | | x | x | | | |
| FPT_SEP.1 | | | | | | | x | x | |

Table11: Security Objectives Coverage for the TOE by the SFR

10.2.1.1 OT.AC_Pers

The security objective **OT.AC_Pers** “Access Control for Personalization and Administration of logical MRTD” addresses the access control of the writing the logical MRTD and the management of the TSF for BAC. The write access to the logical MRTD data are defined by the SFR FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the successfully authenticated Personalization Agents is allowed to write the data of the groups DG1 to DG16 of the logical MRTD only once. So, in phase 4 “Operational Use”, the MRTD Administrator (e.g., in this ST the Personalization Agent acting in phase 4) can add data to the data groups DG3 to DG14, DG16 of the logical MRTD, and update EF.COM, EF.SOD.

The authentication of the terminal as Personalization Agent or as MRTD Administrator shall be performed by TSF according to SRF FIA_UAU.4/MRTD and FIA_UAU.5/MRTD. In case the BAC Authentication Mechanism was used, the SFR FIA_UAU.6/MRTD describes the re-authentication and FDP_UCT.1 and FDP_UTI.1 the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/BAC_MRTD, FCS_COP.1/SHA_MRTD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FCS_CKM.1/PER_MRTD allows to protect the transmitted data by means secure messaging during the personalization process.

The SFR FMT_SMR.1 lists the roles (including Personalization Agent and MRTD Administrator) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization) because the Personalization Agent handles the configuration of the TSF BAC according to the SFR FMT_MOF.1 and the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data if BAC is enabled. The SFR FMT_MTD.1/KEY_READ prevents read access to the Personalization Agent Keys and also to the MRTD Administrator keys and to the BAC Keys, and ensure together with the SFR FPT_EMSEC.1, FPT_FLS.1 and FPT_PHP.3 the confidentiality of these keys.

The SFR FIA_AFL.1 addresses the actions that the TSF shall take in the case of authentication failure.

10.2.1.2 OT.Data_Int

The security objective **OT.Data_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP_ACC.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/PRIM and FDP_ACF.1/BASIC in the same way: only the Personalization Agent is allowed to write the data of the groups DG1 to DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD (cf. FDP_ACF.1.4). Only the MRTD Administrator in phase 4 “Operational Use” (e.g., in this ST the Personalization Agent acting in phase 4) can add data to the data groups DG3 to DG14, DG16 of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent and MRTD Administrator) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization)

If the TOE is configured for the use with Basic Inspection Terminals only by means of FMT_MOF.1 the security objective **OT.Data_Int** “Integrity of personal data” requires the

TOE to ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD. The authentication of the terminal as MRTD Administrator shall be performed by TSF according to SRF FIA_UAU.4/MRTD, FIA_UAU.5/MRTD. The SFR FIA_UAU.6/MRTD, 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/BAC_MRTD (in operational phase), FCS_CKM.1/PER_MRTD (in personalization phase), FCS_COP.1/SHA_MRTD, FCS_RND.1 (for key generation), and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FMT_MTD.1/KEY_WRITE requires the Personalization Agent to establish the Document BAC Keys.

10.2.1.3 OT.Data_Conf

The security objective **OT.Data_Conf** “Confidentiality of personal data” requires the TOE to ensure the confidentiality of the logical MRTD data groups DG1 to DG16 if the TOE is configured for the use with Basic Inspection Systems by means of FMT_MOF.1. The SFR FIA_UID.1 and FIA_UAU.1 allow only those actions before identification respective authentication which do not violate OT.Data_Conf. The read access to the logical MRTD data is defined by the FDP_ACC.1/BASIC and FDP_ACF.1.2/BASIC: only the successful authenticated Personalization Agent, the successful authenticated Basic Inspection System and the successful authenticated MRTD Administrator are allowed to read the data of the logical MRTD. The SFR FMT_SMR.1 lists the roles (including Personalization Agent, Basic Inspection System and MRTD Administrator) 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/MRTD prevents reuse of authentication data to strengthen the authentication of the user. The SFR FIA_UAU.5 enforce the TOE to accept the authentication attempt as Basic Inspection System only by means of the BAC Authentication Mechanism with the Document Basic Access Keys. Moreover, the SFR FIA_UAU.6 request secure messaging after successful authentication of the terminal with BAC 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/TDES_MRTD and FCS_COP.1/MAC_MRTD (cf. the SFR FDP_UCT.1 and FDP_UIT.1) for key generation, and FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD for the ENC_MAC_Mode. The SFR FCS_CKM.1/BAC_MRTD, FCS_CKM.4, FCS_COP.1/SHA_MRTD 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. The SFR FIA_AFL.1 addresses the actions that the TSF shall take in the case of authentication failure.

If the TOE is configured for the use with PIS's, no protection in confidentiality of the logical MRTD is needed to ensure.

10.2.1.4 OT.Identification

The security objective **OT.Identification** “Identification and Authentication of the TOE” address 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.

The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data. The SFR FMT_MTD.1/INI_DIS allow the Personalization Agent to disable Initialization Data because their use in the phase 4 “Operational Use” can violate 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 successfully authentication.

10.2.1.5 OT.Prot_Abuse_Func

The security objective **OT.Prot_Abuse-Func** “Protection against Abuse of Functionality” is ensured by

- the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other which may not be used after TOE Delivery,
- the SFR FPT_RVM.1 which prevents by monitoring the bypass and deactivation of security features or functions of the TOE, and
- the SFR FPT_SEP.1 which prevents change or explore security features or functions of the TOE by means of separation the other TOE functions.

10.2.1.6 OT.Prot_Inf_Leak

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

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMSEC.1,
- by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and
- by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

10.2.1.7 OT.Prot_Phys_Tamper

The security objective **OT.Prot_Phys-Tamper** “Protection against Physical Tampering” is covered by the SFR FPT_PHP.3. The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is covered by:

- 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,
- the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction, and
- the SFR FPT_SEP.1 limiting the effects of malfunctions due to TSF domain separation.

10.2.1.8 OT.Administration

The security objective **OT.Administration** “Security of administrative commands in operational use” requires the TOE to provide secure administrative commands to the MRTD Administrator in phase Operational Use and to prevent the use of these commands from unauthorized users.

The SFRs FCS_CKM.4, FIA_AFL.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.4/MRTD, FIA_UAU.5/MRTD, FMT_MTD.1/KEY_READ, FPT_EMSEC.1 and FPT_RVM.1 prevent the use of administrative commands from unauthorized users. The SFRs FMT_MTD.1/INI_DIS, FDP_ACC.1/PRIM, FDP_ACF.1/PRIM, FDP_ACC.1/BASIC, FDP_ACF.1/BASIC, FMT_MOF.1, FMT_SMF.1, FMT_MTD.1/INI_READ specify this commands.

10.2.2 Security Objectives for the IT Environment

Table12 provides an overview how security functional requirements for the IT environment cover security objectives for the TOE environment. The protection profile describes only those SFR of the IT environment directly related to the SFR for the TOE. It does not state any SFR for the IT environment supporting the security objectives OD.Assurance and OD.Material. The OE.Exam_MRTD uses only security function of the IT environment, i.e. the passive authentication. The security objective OE.Prot_Logical_MRTD is directed to Basic Inspection Systems only which cooperate with the TOE in protection of the logical MRTD.

| | OE.Personalization | OE.Exam_MRTD | OE.Prot_Logical_MRTD | OE.Administration |
|------------------------------|--------------------|--------------|----------------------|-------------------|
| Document Signer | | | | |
| FDP_DAU.1/DS | | x | | |
| Terminal | | | | |
| FCS_CKM.1/BAC_BT | | | x | x |
| FCS_CKM.4/BT | | | x | x |
| FCS_COP.1/SHA_BT | | | x | x |
| FCS_COP.1/ENC_BT | | | x | x |
| FCS_COP.1/MAC_BT | | | x | x |
| FCS_RND.1/BT | | | x | x |
| FIA_UAU.4/BT | | | x | x |
| FIA_UAU.6/BT | | | x | x |
| FDP_UCT.1/BT | | | x | x |
| FDP_UIT.1/BT | | | x | x |
| Personalization Agent | | | | |
| FCS_CKM.1/PT | x | | | |
| FCS_CKM.4/PT | x | | | |
| FCS_COP.1/ENC_PT | x | | | |
| FCS_COP.1/MAC_PT | x | | | |
| FCS_RND.1/PT | x | | | |
| FIA_UAU.4/PT | x | | | |
| FIA_UAU.6/PT | x | | | |
| FDP_UCT.1/PT | x | | | |
| FDP_UIT.1/PT | x | | | |
| FIA_API.1/SYM_PT | x | | | |
| MRTD Administrator | | | | |
| FIA_API.1/SYM_AT | | | | x |

Table12: Security Objectives Coverage for the IT Environment by the SFR

10.2.2.1 OE.Exam_MRTD

The Document Signer, by means of the SFR FDP_DAU.1/DS, shall provide Inspection Systems of Receiving States or Organization with the ability to verify evidence of the validity of the indicated information addressing the security objective **OE.Exam_MRTD**.

10.2.2.2 OE.Prot_Logical_MRTD

The security objective **OE.Prot_Logical_MRTD** “Protection of data of the logical MRTD“ address the protection of the logical MRTD during the transmission and internal handling. The SFRs FIA_UAU.4/BT and FIA_UAU.6/BT address the terminal part of the BAC Authentication Mechanism and FDP_UCT.1/BT and FDP_UIT.1/BT the secure messaging

established by this mechanism. The SFR FCS_CKM.1/BAC_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT are necessary to implement this mechanism. The BIS shall destroy the Document Basic Access Keys and the secure messaging keys after inspection of the MRTD because they are not needed any more. This is addressed by the SFR FCS_CKM.4/BT.

10.2.2.3 OE.Personalization

The **OE.Personalization** “Personalization of logical MRTD” requires the personalization terminal to authenticate themselves to the MRTD’s chip to get the write authorization. This implies to implement the Personalization Agent Authentication Mechanism with the Personalization Agent Authentication Keys or support the symmetric authentication protocol according to the SFR FIA_API.1/SYM_PT.

The SFRs FIA_UAU.4/PT and FIA_UAU.6/PT address the terminal part of the PA Authentication Mechanism and FDP_UCT.1/PT and FDP_UIT.1/PT the secure messaging. The SFR FCS_CKM.1/PT, FCS_COP.1/ENC_PT, FCS_COP.1/MAC_PT and FCS_RND.1/PT are necessary to implement this mechanism. The Personalization terminal shall destroy the AK_{PA} Keys and the secure messaging keys after the personalization of the MRTD because they are not needed any more. This is addressed by the SFR FCS_CKM.4/PT.

10.2.2.4 OE.Administration

The security objective **OE.Administration** “Administration of logical MRTD” requires that the Issuing State or Organization ensure that the MRTD Administrator perform administrative commands with the defined physical and logical security measures.

The SFRs FIA_UAU.4/BT and FIA_UAU.6/BT address the terminal part of the BAC Authentication Mechanism and FDP_UCT.1/BT and FDP_UIT.1/BT the secure messaging established by this mechanism. The SFR FCS_CKM.1/BAC_BT, FCS_COP.1/SHA_BT, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT and FCS_RND.1/BT are necessary to implement this mechanism. The Administration terminal shall destroy the AK_{MA} Keys and the secure messaging keys after inspection of the MRTD because they are not needed any more. This is addressed by the SFR FCS_CKM.4/BT.

The SFR FIA_API.1/SYM_AT insure that this commands are performed by the MRTD Administrator successfully authenticated.

10.3 Dependency Rationale

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

Table13 shows the dependencies between the SFR and of the SFR to the SAR of the TOE.



| SFR | Dependencies | Support of the Dependencies |
|---------------------|---|---|
| FAU_SAS.1 | No dependencies | n.a. |
| FCS_CKM.1/BAC_MRTD | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 1 for non-satisfied dependencies |
| FCS_CKM.1/PER_MRTD | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1/TDES_MRTD, FCS_COP.1/MAC_MRTD justification 1 for non-satisfied dependencies |
| FCS_CKM.4/MRTD | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes | FCS_CKM.1, justification 1 for non-satisfied dependencies |
| FCS_COP.1/SHA_MRTD | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 2 for non-satisfied dependencies |
| FCS_COP.1/TDES_MRTD | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies |
| FCS_COP.1/MAC_MRTD | [FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.1, FCS_CKM.4, justification 3 for non-satisfied dependencies |
| FCS_RND.1/MRTD | No dependencies | n.a. |
| FIA_AFL.1 | FIA_UAU.1 Timing of authentication | Fulfilled |
| FIA_UID.1 | No dependencies | n.a. |
| FIA_UAU.1 | FIA_UID.1 Timing of identification | Fulfilled |
| FIA_UAU.4/MRTD | No dependencies | n.a. |
| FIA_UAU.5/MRTD | No dependencies | n.a. |
| FIA_UAU.6/MRTD | No dependencies | n.a. |
| FDP_ACC.1/PRIM | FDP_ACF.1 Security attribute based access control | Fulfilled by FDP_ACF.1/PRIM |
| FDP_ACC.1/BASIC | FDP_ACF.1 Security attribute based access control | Fulfilled by FDP_ACF.1/BASIC |
| FDP_ACF.1/PRIM | FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization | FDP_ACC.1/PRIM, justification 4 for non-satisfied dependencies |
| FDP_ACF.1/BASIC | FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization | FDP_ACC.1/BASIC, justification 4 for non-satisfied dependencies |
| FDP_UCT.1/MRTD | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/BASIC, justification 5 for non-satisfied dependencies |
| FDP_UIT.1/MRTD | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/BASIC, justification 5 for non-satisfied dependencies |
| FMT_MOF.1 | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FMT_SMF.1 | No dependencies | n.a. |
| FMT_SMR.1 | FIA_UID.1 Timing of identification | Fulfilled |
| FMT_LIM.1 | FMT_LIM.2 | Fulfilled |
| FMT_LIM.2 | FMT_LIM.1 | Fulfilled |

| | | |
|---------------------|---|--|
| FMT_MTD.1/INI_ENA | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FMT_MTD.1/INI_DIS | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FMT_MTD.1/INI_READ | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FMT_MTD.1/KEY_WRITE | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FMT_MTD.1/KEY_READ | FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles | Fulfilled |
| FPT_EMSEC.1 | No dependencies | n.a. |
| FPT_FLS.1 | ADV_SPM.1 | Fulfilled by EAL4 |
| FPT_PHP.3 | No dependencies | n.a. |
| FPT_RVM.1 | No dependencies | n.a. |
| FPT_SEP.1 | No dependencies | n.a. |
| FPT_TST.1 | FPT_AMT.1 Abstract machine testing | See justification 6 for non-satisfied dependencies |

Table13: Dependencies between the SFR for the TOE

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

1. The SFR FCS_CKM.1/BAC_MRTD uses only the Document Basic Access Keys to generate the secure messaging keys used for FCS_COP.1/TDES and FCS_COP.1/MAC while FCS_CKM.1/PER_MRTD uses the AK_{MA} keys. The SFR FCS_CKM.4/MRTD destroys these keys automatically. These simple processes do not need any special security attributes for the secure messaging keys.
2. The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR are needed to be defined for this specific instantiation of FCS_COP.1.
3. The SFR FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD use the automatically generated secure messaging keys assigned to the session with the successfully authenticated BIS only. There is no need for any special security attributes for the secure messaging keys.
4. 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.2) is necessary here.
5. The SFR FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the use secure messaging between the MRTD and the BIS. There is no need for additional SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels it is the only one.
6. The TOE consists of the software and its underlying hardware on which it is running. Thus there is no abstract machine to be tested.

Table14 illustrates the dependencies between the SFR for the IT environment and of the SFR to the SAR of the TOE.



| SFR | Dependencies | Support of the Dependencies |
|------------------|--|---|
| FDP_DAU.1 | No dependencies | n.a. |
| FCS_CKM.1/BAC_BT | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1/ENC_BT, FCS_COP.1/MAC_BT justification 7 for non-satisfied dependencies |
| FCS_CKM.4/BT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes | FCS_CKM.1, justification 7 for non-satisfied dependencies |
| FCS_COP.1/SHA_BT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security Attributes | FCS_CKM.1, FCS_CKM.4, justification 8 for non-satisfied dependencies |
| FCS_COP.1/ENC_BT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 cryptographic key destruction, FMT_MSA.2 Secure security Attributes | FCS_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies |
| FCS_COP.1/MAC_BT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 cryptographic key destruction, FMT_MSA.2 Secure security Attributes | FCS_CKM.1, FCS_CKM.4, justification 9 for non-satisfied dependencies |
| FCS_RND.1/BT | No dependencies | n.a. |
| FIA_UAU.4/BT | No dependencies | n.a. |
| FIA_UAU.6/BT | No dependencies | n.a. |
| FDP_UCT.1/BT | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies |
| FDP_UIT.1/BT | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies |
| FCS_CKM.1/PT | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes | FCS_CKM.4, FCS_COP.1/ENC_PT, FCS_COP.1/MAC_PT justification 11 for non-satisfied dependencies |
| FCS_CKM.4/PT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FMT_MSA.2 Secure security attributes | FCS_CKM.1, justification 11 for non-satisfied dependencies |
| FCS_COP.1/ENC_PT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 cryptographic key destruction, FMT_MSA.2 Secure security Attributes | FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies |
| FCS_COP.1/MAC_PT | [FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 cryptographic key destruction, FMT_MSA.2 Secure security Attributes | FCS_CKM.1, FCS_CKM.4, justification 12 for non-satisfied dependencies |
| FCS_RND.1/PT | No dependencies | n.a. |
| FIA_UAU.4/PT | No dependencies | n.a. |
| FIA_UAU.6/PT | No dependencies | n.a. |
| FDP_UCT.1/PT | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies |
| FDP_UIT.1/PT | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or | FDP_ACC.1/BASIC, justification 10 for non-satisfied dependencies |

| | | |
|------------------|--|------|
| | FDP_IFC.1 Subset information flow control] | |
| FIA_API.1/SYM_PT | No dependencies | n.a. |
| FIA_API.1/SYM_AT | No dependencies | n.a. |

Table14: Dependencies between the SFR for the IT Environment

Justification for non-satisfied dependencies between the SFR for the IT environment:

7. The SFR FCS_CKM.1/BAC_BT derives the Document Basic Access Keys and uses these keys to generate the secure messaging keys used for FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD. The SFR FCS_CKM.4/PT destroys these keys. These processes do not need any special security attributes for the secure messaging keys. Note that the encryption cryptographic operation addressed by FCS_COP.1/ENC_BT allows the MRTD Administrator to derive the seed key for the AK_{MA} keys.
8. The cryptographic algorithm SHA-1 does not use any cryptographic key. Therefore none of the listed SFR is needed to be defined for this specific instantiation of FCS_COP.1.
9. The SFR FCS_COP.1/ENC_BT and FCS_COP.1/MAC_BT use the automatically generated secure messaging keys assigned to the session with the successfully authenticated MRTD only. There is no need for any special security attributes for the secure messaging keys.
10. The SFR FDP_UCT.1/MRTD and FDP_UTI.1/MRTD require the use secure messaging between the MRTD and the BIS/PT. There is no need to provide further description of this communication.
11. The SFR FCS_CKM.1/PT derives the AK_{PA} keys and uses these keys to generate the secure messaging keys used for FCS_COP.1/ENC_PT and FCS_COP.1/MAC_PT. The SFR FCS_CKM.4/PT destroys these keys after personalization.
12. The SFR FCS_COP.1/ENC_PT and FCS_COP.1/MAC_PT use the secure messaging keys assigned to the session with the successfully authenticated Personalization Agent. There is no need for any special security attributes for the secure messaging keys.

10.4 Security Assurance Requirements Rationale

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

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the MRTD's chip especially for the absence of unintended functionality.

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

The minimal strength of function "high" was selected to ensure resistance against direct attacks on functions based on probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE to fulfil OT.AC_PERS, OT.Administration and OT.Data_Conf if the TOE is configured for the use with Basic Inspection Systems. This is consistent with the security objective OD.Assurance.

The components ADV_IMP.2 and ALC_DVS.2 augmented to EAL4 have dependencies to other security requirements fulfilled within EAL4

Dependencies ADV_IMP.2: ADV_LLD.1 Descriptive low-level design
 ALC_TAT.1 Well-defined development tools

Dependencies ALC_DVS.2: None

10.5 Security Requirements – Mutual Support and Internal Consistency

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

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

the dependency analysis in section 10.3 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

the assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the additional assurance components in section 10.4 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

The Personalization Agent may configure the TOE according to the organisational security policy (i) for use with Primary Inspection Systems or (ii) for use with Basic Inspection Systems. According to the security objective OT.Data_Conf the TOE enforces different security functional policies for the chosen (by means of the SFR FMT_MOF.1) configurations (i.e. the Primary Access Control SFP for the use with Primary Inspection

Systems and the Basic Access Control SFP for the use with Basic Inspection Systems). These SFP are implemented by two internally consistent sets of SFR for the cryptographic functions, the user identification, the user authentication, the access control and - in case of the Basic Access Control SFP – for the data export protection. All TSF are protected by a common set of SFR of the FPT against any attempt to bypass, to deactivate, to manipulate or to misuse the TOE security features or TSF.

Inconsistency between functional and assurance requirements could only arise if there are functional assurance dependencies which are not met, a possibility which has been shown not to arise in section 10.3 Dependency Rationale and 10.4 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 10.4 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.