# Public Security Target CombICAO Applet v3 on ID-One Cosmo X EAC Configuration

Reference: FQR 550 0283 Ed 6

# DOCUMENT EVOLUTION

| Date | Version | Name | Revision |
|---|---|---|---|
| 29/11/2021 | Ed 1 | IDEMIA | Sanitized version created for Public Issue. |
| 01/02/2022 | Ed 2 | IDEMIA | Sanitized version created for Public Issue after incorporating ANSSI feedbacks. |
| 16/01/2023 | Ed 3 | IDEMIA | Update [AGD_PRE], [AGD_OPE], [ST_PTF] and [PTF_CERT] references |
| 28/03/2023 | Ed 4 | IDEMIA | Update [PTF_CERT] and [ST_PTF] references. |
| 19/07/2023 | Ed 5 | IDEMIA | Update [PTF_CERT] and [ST_PTF] references.<br>Add ALC_FLR.1 |
| 19/01/2026 | Ed 6 | INSI | Updates for re-evaluation 2025 |

# Table of contents

Table of figures

# Table of tables

# 1 Security Target Introduction

## 1.1 ST Identification

| | |
|---|---|
| **Title** | CombICAO Applet v3 in EAC configuration on ID-One Cosmo X Public Security Target |
| **ST Identification** | FQR 550 0283 Ed 6 |
| **CC Version** | 3.1 revision 5 |
| **Assurance Level** | EAL5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5 |
| **ITSEF** | CEA-LETI |
| **Certification Body** | ANSSI |
| **Compliant to Protection Profile** | [PP_EAC] |

## 1.2 TOE Reference

| | |
|---|---|
| **TOE Commercial Name** | CombICAO Applet v3 in EAC configuration on ID-One Cosmo X |
| **Applet Code Versions (SAAAAR Code)** | '20 37 42 FF' |
| **Applet Internal Version** | '00 00 02 0D' |
| **Platform Name** | ID-One Cosmo X |
| **Platform Certificate** | [PTF_CERT] |
| **Guidance Documents** | [AGD_PRE], [AGD_OPE]. |

# 2 Technical Terms, Abbreviations and Associated References

## 2.1 Technical Terms

| Term | Definition |
|---|---|
| *Accurate Terminal Certificate* | A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [TR-03110-3]. |
| *Advanced Inspection Procedure (with PACE)* | A specific order of authentication steps between a travel document and a terminal as required by [TR-03110-3], namely (i) PACE, (ii) Chip Authentication v1, (iii) Passive Authentication with $SO_D$ and (iv) Terminal Authentication v1. AIP can generally be used by EIS-AIP-PACE. |
| *Agreement* | This term is used in the current ST in order to reflect an appropriate relationship between the parties involved, but not as a legal notion. |
| *Application note* | Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7). |
| *Audit records* | Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data. |
| *Authenticity* | Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organization |
| *Basic Access Control* | Security mechanism defined in [ICAO_9303] by which means the travel document's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there). |
| *Basic Inspection System (BIS)* | A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). |
| *Biographical data (bio data).* | The personalised details of the bearer of the travel document appearing as text in the visual and machine readable zones on the biographical data page of a travel document [ICAO_9303]. |
| *Biometric reference data* | Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data. |

| Term | Definition |
|---|---|
| *Card Access Number (CAN)* | Password derived from a short number printed on the front side of the data-page. |
| *Certificate chain* | A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. |
| *Counterfeit* | An unauthorized copy or reproduction of a genuine security document made by whatever means. |
| *Country Signing CA Certificate ($C_{CSCA}$)* | Self-signed certificate of the Country Signing CA Public Key ($K_{Pu\ CSCA}$) issued by CSCA stored in the inspection system. |
| *Country Signing Certification Authority (CSCA)* | An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI.<br><br>The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [ICAO_9303], 5.5.1.<br><br>The Country Signing Certification Authority issuing certificates for Document Signers (cf. [6]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3]. |
| *Country Verifying Certification Authority (CVCA)* | An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [TR-03110-3].<br><br>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this ST.<br><br>The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [ICAO_9303]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [TR-03110-3]. |

| Term | Definition |
|---|---|
| *Current date* | The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates. |
| *CV Certificate* | Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key. |
| *CVCA link Certificate* | Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key. |
| *Document Basic Access Key Derivation Algorithm* | The [ICAO_9303] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data. |
| *Document Details Data* | Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data. |
| *Document Basic Access Keys* | Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the travel document's chip and the inspection system [ICAO_9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book. |
| *Document Security Object ($SO_D$)* | A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (CDS). [ICAO_9303] |
| *Document Signer (DS)* | An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication.<br><br>A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS), see [ICAO_9303].<br><br>This role is usually delegated to a Personalisation Agent. |
| *Document Verifier (DV)* | An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, |

| Term | Definition |
|---|---|
| | see [TR-03110-3].<br><br>Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this ST.<br><br>There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy) [1] [2] |
| *Eavesdropper* | A threat agent with low attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip. |
| *Enrolment* | The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [ICAO_9303] |
| *travel document (electronic)* | The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport. |
| *ePassport application* | [PP-EAC] definition<br>Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes<br>the file structure implementing the LDS [ICAO_9303],<br>the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and<br>the TSF Data including the definition the authentication data but except the authentication data itself. |
| *Extended Access Control* | Security mechanism identified in [ICAO_9303] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalisation Agent may use the same mechanism to authenticate themselves with Personalisation Agent Authentication Private Key and to get write and read access to the |

[1] The form of such an agreement may be of formal and informal nature; the term 'agreement' is used in the current ST in order to reflect an appropriate relationship between the parties involved.

[2] Existing of such an agreement may be technically reflected by means of issuing a CCVCA-F for the Public Key of the foreign CVCA signed by the domestic CVCA.

| Term | Definition |
|---|---|
| | logical travel document and TSF data. |
| *Extended Inspection System (EIS)* | A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism. |
| *Forgery* | Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. |
| *Global Interoperability* | The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel document's. [ICAO_9303] |
| *IC Dedicated Software* | Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases. |
| *IC Dedicated Support Software* | That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases. |
| *IC Dedicated Test Software* | That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter. |
| *IC Embedded Software* | Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE. |
| *IC Identification Data* | The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. |
| *Impostor* | A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. |
| *Improperly documented person* | A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [ICAO_9303] |

| Term | Definition |
|---|---|
| *Initialisation* | Process of writing Initialisation Data (see below) to the TOE (TOE life-cycle, Phase 2 Manufacturing, Step 3). |
| *Initialisation Data* | Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document material (IC identification data). |
| *Inspection* | The act of a State examining an travel document presented to it by a traveller (the travel document's holder) and verifying its authenticity. [ICAO_9303] |
| *Inspection system (IS)* | A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder. |
| *Integrated circuit (IC)* | Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit. |
| *Integrity* | Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by the issuing State or Organization |
| *Issuing Organization* | Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO_9303]] |
| *Issuing State* | The Country issuing the travel document. [ICAO_9303] |
| *Logical Data Structure (LDS)* | The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the travel document's chip. |
| *Logical Data Structure 2 (LDS2)* | The file structures required to support the ICAO LDS2 [9303-10_LDS2] consisting of LDS file structure with three additional and optional applications:<br>• Travel records (stamps);<br>• Visa records; and<br>• Additional biometrics. |

| Term | Definition |
|---|---|
| *Logical travel document* | Data of the travel document holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to)<br>personal data of the travel document holder<br>the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),<br>the digitized portraits (EF.DG2),<br>the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and<br>the other data according to LDS (EF.DG5 to EF.DG16).<br>EF.COM and EF.SOD |
| *Machine Readable Travel Document (MRTD)* | Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO_9303] |
| *Machine Readable Zone (MRZ)* | Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [ICAO_9303]. |
| *Machine-verifiable biometrics feature* | A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [ICAO_9303] |
| *Manufacturer* | Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. |
| *Metadata of a CV Certificate* | Data within the certificate body (excepting Public Key) as described in [TR-03110-3].<br>The metadata of a CV certificate comprise the following elements:<br>- Certificate Profile Identifier,<br>- Certificate Authority Reference,<br>- Certificate Holder Reference,<br>- Certificate Holder Authorisation Template,<br>- Certificate Effective Date,<br>- Certificate Expiration Date. |
| *Optional biometric reference data* | Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (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. |

| Term | Definition |
|---|---|
| *Password Authenticated Connection Establishment (PACE)* | A communication establishment protocol defined in [ICAO_9303] part 11. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained. |
| *PACE passwords* | Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [ICAO_9303] part 11 or a user PIN or PUK as specified in [TR-03110-3] |
| *Passive authentication* | (i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object. |
| *Personalisation* | The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. paragraph 1.7.4.3, TOE life-cycle, Phase 3, Step 6). |
| *Personalisation Agent* | An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities:<br>ICAO travel document<br>(i) establishing the identity of the travel document holder for the biographic data in the travel document,<br>(ii) enrolling the biometric reference data of the travel document holder,<br>(iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [TR-03110-1],<br>(iv) writing the document details data,<br>(v) writing the initial TSF data,<br>(vi) signing the Document Security Object defined in [ICAO_9303] (in the role of DS).<br><br>Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer.<br><br>Generating signature key pair(s) is not in the scope of the tasks of this role. |
| *Personalisation Data* | A set of data incl.<br>individual-related data (biographic and biometric data) of the travel document holder,<br>dedicated document details data and |

| Term | Definition |
|---|---|
| | dedicated initial TSF data (incl. the Document Security Object).<br><br>Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing. |
| *Personalisation Agent Authentication Information* | TSF data used for authentication proof and verification of the Personalisation Agent. |
| *Personalisation Agent Key* | Symmetric cryptographic key or key set (MAC, ENC) used by the Personalisation Agent to prove his identity and get access to the logical travel document. |
| *Physical part of the travel document* | travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to)<br>biographical data,<br>data of the machine-readable zone,<br>photographic image and<br>other data. |
| *Pre-personalisation* | Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (TOE life-cycle, Phase 2, Step 5) |
| *Pre-personalisation Data* | Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair and Chip Life-Cycle Production data (CPLC data). |
| *Pre-personalised travel document's chip* | travel document's chip equipped with a unique identifier. |
| *Receiving State* | The Country to which the travel document holder is applying for entry. [ICAO_9303] |
| *Reference data* | Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt. |
| *RF-terminal* | A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443]. |
| *Secondary image* | A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means [ICAO_9303]. |

| Term | Definition |
|---|---|
| *Secure messaging in encrypted /combined mode* | Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816] |
| *Service Provider* | An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. |
| *Skimming* | Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data. |
| *Standard Inspection Procedure* | A specific order of authentication steps between an travel document and a terminal as required by [ICAO_9303] and [TR-03110-1], namely PACE or BAC and Passive Authentication with $SO_D$. |
| *Inspection Procedure for multi-application travel document's* | This section describes an inspection procedure designed for travel document's containing one or more applications besides the travel document's application ("LDS2-documents"): [LDS2_TR] Annex A2. |
| *Terminal* | A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.<br><br>In this ST the role 'Terminal' corresponds to any terminal being authenticated by the TOE. |
| *Terminal Authorization* | Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date. |
| *Terminal Authorisation Level* | Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date. |
| *TOE tracing data* | Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document. |
| *travel document* | Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [ICAO_9303] (there "Machine readable travel document"). |
| *travel document (electronic)* | The contact based or contactless smart card integrated into the plastic or paper, optical readable cover and providing the following application: *ePassport*. |
| *travel document Holder* | The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document. |

| Term | Definition |
|---|---|
| *travel document's Chip* | A contact based / contactless integrated circuit chip complying with ISO/IEC 14443 [15] and programmed according to the Logical Data Structure as specified by ICAO, [ICAO_9303], sec III. |
| *Traveller* | Person presenting the travel document to the inspection system and claiming the identity of the travel document holder. |
| *TSF data* | Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [CC1]). |
| *Unpersonalised travel document* | The travel document that contains the travel document chip holding only Initialisation Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer. |
| *User data* | All data (being not authentication data)<br>stored in the context of the ePassport application of the travel document as defined in [5] and<br>being allowed to be read out solely by an authenticated terminal.<br><br>CC give the following generic definitions for user data:<br>Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC2]). |
| *Verification* | The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303] |
| *Verification data* | Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity. |

## 2.2 Abbreviations

| Acronym | Definition |
|---|---|
| BAC | Basic Access Control |
| BAP | Basic Access Protection |
| BIS | Basic Inspection System |
| CA | Chip Authentication |
| CAN | Card Access Number |
| CC | Common Criteria |
| CLFDB | Ciphered Load File Data Block |
| DER | Distinguished Encoding Rules |
| DES | Data Encryption Standard |
| DF | Dedicated File |
| DH | Diffie Hellman |
| DSK | Dump Secret Key |
| EAC | Extended Access Control |
| EAL | Evaluation Assurance Level |
| EF | Elementary File |
| FID | File identifier |
| GP | Global Platform |
| IC | Integrated Chip |
| ICAO | International Civil Aviation Organization |
| ICC | Integrated Chip card |
| ICCSN | Integrated Circuit Card Serial Number. |
| IFD | Interface Device |
| IS | Inspection System |
| IDL | ISO-compliant Driving Licence |
| LSK | Load Secure Key |
| MAC | Message Authentication code |
| MF | Master File |
| MRTD | Machine Readable Travel Document |
| MRZ | Machine readable zone |
| OE | Security Objectives for the Operational Environment |
| OSP | Organisational security policy |
| OT | Security Objectives for the TOE |
| PACE | Password Authenticated Connection Establishment |
| PCD | Proximity Coupling Device |
| PICC | Proximity Integrated Circuit Chip |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |

| | |
|---|---|
| PS | Personalisation System |
| PT | Personalisation Terminal |
| RF | Radio Frequency |
| ROM | Read Only Memory |
| RSA | Rivest Shamir Adleman |
| RSA CRT | Rivest Shamir Adleman – Chinese Remainder Theorem |
| SAI | Scanning Area Identifier |
| SAR | Security Assurance Requirement |
| SCP | Secure Channel Procotol |
| SFR | Security functional requirement |
| SHA | Secure Hashing Algorithm |
| SIP | Standard Inspection Procedure |
| ST | Security Target |
| TA | Terminal Authentication |
| TOE | Target Of Evaluation |
| TSF | TOE Security Functions |

## 2.3 References

| Reference | Description |
|---|---|
| [ADDENDUM] | 20190821-Module-PP0056 - v1.1 |
| [AGD_OPE] | FQR 220 1641 Ed 4 - CombICAO Applet V3 on ID-One Cosmo X - AGD_OPE |
| [AGD_PRE] | FQR 220 1640 Ed 4 - CombICAO Applet V3 on ID-One Cosmo X - AGD_PRE |
| [CC1] | Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1. Revision 5. April 2017. CCMB-2017-04-001. |
| [CC2] | Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-002. |
| [CC3] | Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements. Version 3.1. Revision 5. April 2017. CCMB-2017-04-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1. Revision 5. April 2017. CCMB-2017-04-004. |
| [FIPS_180_4] | FIPS 180-4, Federal Information Processing Standards Publication (FIPS PUB) 180-4, Secure Hash Standard, August 2015 |
| [FIPS_186_3] | FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009 |
| [FIPS_197] | FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES) |
| [FIPS_46_3] | FIPS 46-3, Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard (DES), 1999 October 25 |
| [GPC_SPE_014] | GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.3 – Amendment D" Version 1.1.2 - Public Release March 2019 |
| [GPC_SPE_034] | "GlobalPlatform Card Specification" Version 2.3.1 Public Release - March 2018 |

| Reference | Description |
|---|---|
| [ICAO_9303] | International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – 7th and 8th edition. |
| [ISO_15946] | ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002 |
| [ISO_18013-3] | ISO/IEC 18013-3: Information technology — Personal identification — ISO-compliant driving licence. Part 3: Access control, authentication and integrity validation, April 2017. |
| [ISO_TR_19446] | ISO/IEC TR 19446:2015<br>Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications |
| [ISO_9796-2] | ISO/IEC 9796-2:2002 - Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash-function |
| [ISO_9797_1] | ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication codes (MACs) – part 1: Mechanisms using a block cipher, Second edition 2011-03-01 |
| [ISO11770-2] | ISO/IEC 11770-2. Information Technology – Security techniques – Key management – part 2: Mechanisms using symmetric techniques, 1996 |
| [ISO11770-3] | ISO/IEC 11770-3. Information Technology – Security techniques – Key management – part 3: Mechanisms using asymmetric techniques, 2015 |
| [ISO14443] | ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016 |
| [ISO7816] | ISO/IEC 7816: Identification cards — Integrated circuit cards. |
| [NIST_800_38A] | NIST Special Publication 800-38A: 2001, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001 |
| [NIST_800_38B] | NIST Special Publication 800-38B: 2005, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005 |
| [PKCS#3] | PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4 Revised November 1, 1993 |

| Reference | Description |
|---|---|
| [PP_BAC] | Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009 |
| [PP_EAC] | EAC- Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009 |
| [PP_EACwPACE] | Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), BSI-CC-PP0056-V2-2012-MA-02, version 1.3.2, 5th December 2012 |
| [PP_IC] | Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014. |
| [PP_PACE] | Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011-MA-01, Version 1.01, 22 July 2014 |
| [PP-SSCD2] | Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016 |
| [PP-SSCD3] | Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, June 30 2016 |
| [PP-SSCD4] | Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, CEN/TC 224, BSI-CC-PP-0071-2012-MA-01, Version 1.0.1, June 30 2016 |
| [PP-SSCD5] | Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, EN 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, June 30 2016 |
| [PP-SSCD6] | Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application, EN 419211-6:2013, CEN/TC 224, BSI-CC-PP-0076-2013-MA-01, Version 1.0.4, June 30 2016 |
| [PTF_CERT] | ANSSI-CC-2023/06-R01 - 18/12/2024 |

| Reference | Description |
|---|---|
| [ST_PTF] | Security Target Lite ID-ONE Cosmo X,<br>FQR 110 A19A Ed 3 |
| [QR_Guide] | FQR 220 1646 Ed 1 - CombICAO Applet V3 -<br>Recommendations for Compatibility with QR |
| [RGS2_B1] | GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES, Version 2.04 du 01 Janvier 2020 |
| [TR-03110-1] | Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015 by BSI |
| [TR-03110-2] | Technical Guideline TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Version 2.21, 21.12.2016 by BSI |
| [TR-03110-3] | TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3: Common Specifications, version 2.21, 21-12-2016 by BSI |
| [TR-03111] | Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, Version 1.11, 17.04.2009 |
| [X9.62] | AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry (rDSA), 9 september 1998 |

# 3 TOE Overview and Description

## 3.1 TOE Overview

The TOE is a composite product that consist of an INSI applet named CombICAO v3 loaded on IDEMIA ID-One Cosmo X Global Platform and Java Card Operating system. The product is contact and/or contactless smart card security controller in **EAC configuration** Products.

It supports the ICAO and [TR-03110-1] and [TR-03110-3] defined protocols for EACv1 (Chip Authentication v1 and Terminal Authentication v1) and Active Authentication (AA).

This Security Target addresses the protection of the logical travel document
(i) in integrity by write-only-once access control and by physical means, and
(ii) in confidentiality with the Extended Access Control Mechanism.

TOE implements the Extended Access Control as defined in [TR-03110-1] and [TR-03110-3].

The Extended Access Control consists of two parts
(i) Chip Authentication Protocol Version 1 (v1), and
(ii) Terminal Authentication Protocol Version 1 (v1).

Chip Authentication acts as an alternative to the Active Authentication stated in [ICAO_9303].

The Chip Authentication Protocol v1
(i) authenticates the travel document's chip to the inspection system and
(ii) establishes secure messaging which will be used by Terminal Authentication v1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the Extended Inspection System. Therefore Terminal Authentication v1 can only be performed if Chip Authentication v1 has been successfully executed.

The Terminal Authentication Protocol v1 consists of
(i) the authentication of the Extended Inspection System as entity authorized by the receiving State or Organisation through the issuing State, and
(ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

Within the scope of this ST, the TOE can be configured as a stand-alone application or as a combination of the following official ID document applications:
- ICAO/EAC eMRTD and
- EU/ISO Driving Licence compliant to [ISO_18013-3] or [ISO_TR_19446].

The TOE may be used as an ISO Driving Licence (IDL) as both eMRTD and IDL applications share the same protocols and data structure organization

The CombICAO Applet v3 is also evaluated in other configurations as mentioned in the Table below.

This ST considers the CombICAO Applet v3 in the **EAC configuration**.

| Configuration | PP Conformity | Extensions to the PP |
|---|---|---|
| BAC and CA | [PP_BAC] | - Active Authentication (AA)<br>- Chip Authentication Protocol (v1)<br>- Restart secure messaging in AES128, AES192 or AES256 secure messaging (in addition to 3DES) after Chip Authentication Protocol (v1) |
| **EAC in combination with BAC** | **[PP_EAC]** | - **Active Authentication (AA)**<br>- **Enhanced protection over Sensitive biometric data reading** |
| EAC with PACE | [PP_PACE] | - Active Authentication (AA)<br>- PACE-CAM (Optional)<br>- Automatic BAC phasing out<br>- Enhanced protection over Sensitive biometric data reading |
| | [PP_EACwPACE] | |
| EAC with PACE for French ID | [PP_PACE] | - [ADDENDUM]<br>- Active Authentication (AA)<br>- PACE-CAM (Optional)<br>- Automatic BAC phasing out<br>- Enhanced protection over Sensitive biometric data reading |
| | [PP_EACwPACE] | |
| SSCD | [PP-SSCD2], [PP-SSCD3], [PP-SSCD4], [PP-SSCD5], and [PP-SSCD6] | - ADMIN role<br>- Integrity token |

**Table 1 Different evaluated configurations of the CombICAO application**

## 3.2 TOE Description

The TOE in the EAC configuration encompasses the following features:

- In Personalisation phase:
  - authentication protocol for personalisation agent authentication;
  - 3DES, AES128, AES192 and AES256 Global Platform secure messaging;
  - access control;
  - Creation and configuration of application instances and their logical data structure;
  - Secure data loading;
  - Secure import and/or on-chip generation of Chip Authentication key pairs for CAv1;
  - Secure import and/or on-chip generation of the AA key pair;
  - life-cycle phase switching to operational phase;

- In operational phase:
  - EAC: Chip Authentication v1 (CAv1) and Terminal Authentication v1 (TAv1);
  - Active Authentication (AA);
  - After CAv1: restart ICAO secure messaging in 3DES, AES128, AES192 or AES256 cipher mode;
  - After EAC: access control to DG3 and DG4 based on the effective authorization established during TAv1;
  - Automatic BAC phasing out;
  - CA Key Renewal;
  - Key Usage Counter;

### *3.2.1 Physical scope of the TOE*

The TOE is physically made up of several components hardware and software.
Once constructed, the TOE is a bare microchip with its external interfaces for communication.

The TOE may be used on several physical medium like wafer, inlay, eCover, eDatapage, eMRTD booklet or in a smart card.

The physical medium on which the microchip is mounted is not part of the target of evaluation as it does not alter nor modify any security functions of the TOE. Also, the inlay production including the application of the antenna is not part of the TOE

### *3.2.2 Logical scope of the TOE*

The TOE is a smartcard, composed of:

- IC,
- Java Card Open Platform (OS) and
- CombICAO Applet v3 (data storage file structure)

The pre-personalisation and personalisation are performed by the Manufacturer and the Personalisation Agent, which controls the TOE. All along this phase, the TOE is self-

protected, as it requires the authentication of the Manufacturer and the Personalisation Agent prior to any operation.

By being authenticated, the Personalisation Agent gets the rights (access control) for
(1) reading and writing data,
(2) instantiating the application, and
(3) writing of personalisation data. The Personalisation Agent can so create the file structure (MF / ADF) required for this configuration.

A schematic overview of the TOE's logical architecture is shown in below figure:

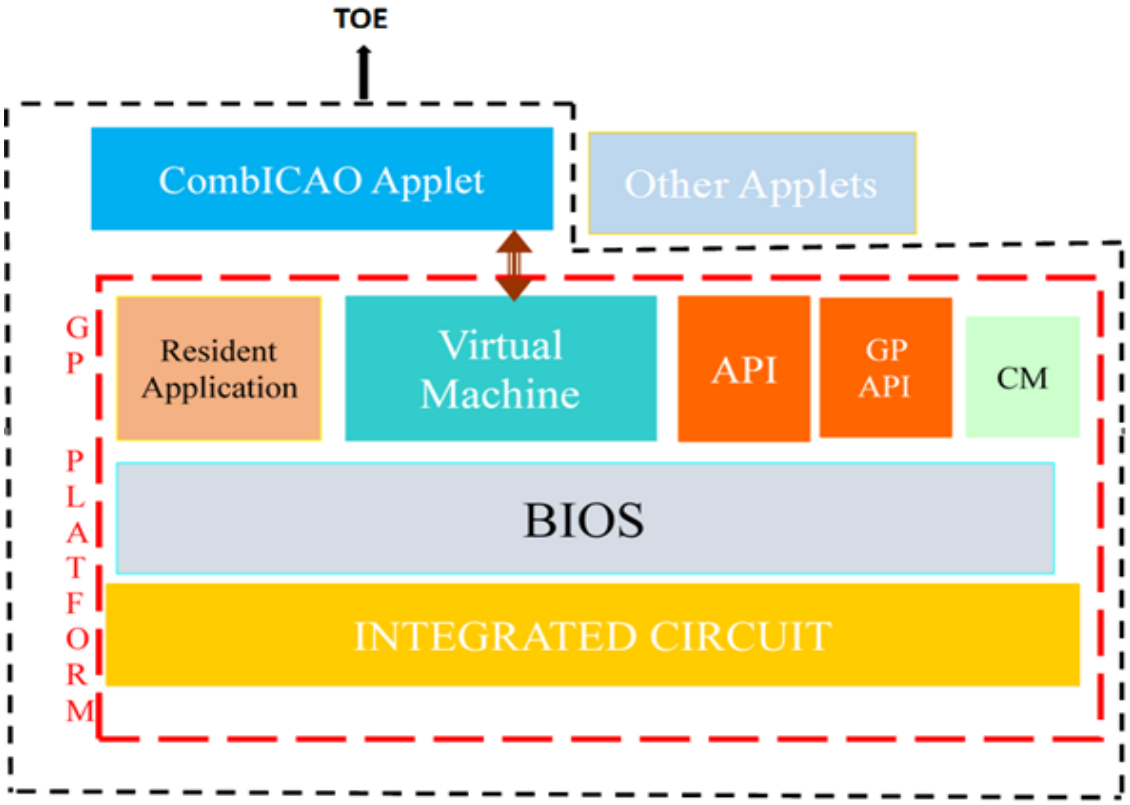



**Figure 1 TOE's logical architecture**

The TOE is composed of:

- Circuitry of the MRTD's chip (the IC) :
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- ID-One Cosmo X Platform: see [ST_PTF] and [PTF_CERT]
- CombICAO Applet v3
- Associated guidance documentation (delivered in electronic version).

The following guidance documents will be provided with the TOE:

| Guidance | Audience | Form Factor of Delivery |
|---|---|---|
| [AGD_PRE] | Personalising Agent | Electronic Version |
| [AGD_OPE] | End user of the TOE | |

The following guide is provided only in case compliancy with QR scheme is required:

| Guidance | Purpose | Form Factor of Delivery |
|---|---|---|
| [QR_Guide] | Recommendations for QR | Electronic Version |

An ST Lite version of this Security Target will also be provided along with above-mentioned documents.

Platform related guidance documents are mentioned in [ST_PTF].

"Life Cycle" section in this ST provides more details about the TOE delivery for the different options.

## 3.3 Required non-TOE hardware/Software/firmware

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

**Note**: In particular, the TOE may be used in contact mode, without any inlay or antenna.

## 3.4 TOE Usage and major security features of the TOE

A State or Organization issues MRTDs to be used by the holder for international travel. The travel document presenter presents a MRTD to the inspection system to prove his or her identity.

The MRTD in context of this Security Target contains

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

The authentication of the travel document presenter is based on (i) the possession of a valid MRTD personalised for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

The MRTD is viewed as unit of

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

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

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

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational

security measures (e.g. control of materials, personalisation procedures) [ICAO_9303]. These security measures include the binding of the MRTD's chip to the passport book.

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

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

**Mutatis mutandis**, the TOE may also be used as an ISO driving licence, compliant to [ISO_18013-3] or [ISO_TR_19446] supporting BAP-1 (the same protocol as BAC but used in the context of driving licence), AA and CA, as both applications (MRTD and IDL) share the same protocols and data structure organization. Therefore, in the rest of the document, the word "MRTD" MAY be understood either as a MRTD in the sense of ICAO, or a driving licence compliant to [ISO_18013-3] or [ISO_TR_19446] depending on the targeted usage envisioned by the issuer.

The table below indicates how terms and concept present in the current document shall be read, when considering the TOE to be an ISO driving licence:

| MRTD | ISO-compliant Driving Licence |
|---|---|
| MRTD | IDL |
| ICAO | ISO/IEC |
| ICAO 9303 | [ISO_18013-3] or [ISO_TR_19446] |
| BAC | BAP-1 |
| DG3 | DG7 |
| DG4 | DG8 |
| DG15 | DG13 |
| MRZ or CAN | MRZ or SAI |
| Traveller | Holder |

### *3.4.1 Active Authentication (AA)*

Active Authentication is an authentication mechanism ensuring the chip is genuine. It uses a challenge-response protocol between the IS and the chip.
Active Authentication is realised with the INTERNAL AUTHENTICATE command. The key and algorithms supported are the following:

RSA ISO/IEC 9796-2 with a key length of 1024, 1536, 2048, 3072 and 4096 bits and hashing algorithm of SHA1 or SHA2 (i.e. SHA256, SHA384 and SHA512).

ECDSA over prime field curves with hashing algorithm of SHA1 or SHA2 (i.e. SHA256, SHA384 and SHA512) and the key sizes 192 to 521.

### 3.4.2 Basic Access Control (BAC)

The protocol for Basic Access Control is specified by [ICAO_9303]. Basic Access Control checks that the terminal has physical access to the MRTD's data page. This is enforced by requiring the terminal to derive an authentication key from the optically read MRZ of the MRTD. The protocol for Basic Access Control is based on [ISO11770-2] key establishment mechanism 6. This protocol is also used to generate session keys that are used to protect the confidentiality (and integrity) of the transmitted data.

The Basic Access Control (BAC) is a security feature that is supported by the TOE. The inspection system reads the printed data on the document (MRZ), authenticates itself as inspection system by means of keys derived from MRZ data. After successful 3DES based authentication, the TOE provides read access to data requiring BAC rights by means of a private communication (secure messaging) with the inspection system.

The purpose of this mechanism is to ensure that the holder gives access to the IS to the logical MRTD (data stored in the chip); It is achieved by a mutual authentication.

Once the mutual authentication is performed, a secure messaging is available to protect the communication between the chip and the IS.

This table lists the supported configurations for BAC protocol:

| Configuration | Key Algo | Key Length | Hash Algo | MAC Algo |
|---|---|---|---|---|
| BAC | 3DES 2Key | 16-bytes | SHA-1 | Retail MAC |

**Table 2 BAC Configuration**

### 3.4.3 Chip Authentication Protocol (v1)

The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the MRTD chip.

The protocol establishes Secure Messaging between an MRTD chip and a terminal based on a static key pair stored on the MRTD chip. Chip Authentication is an alternative to the optional ICAO Active Authentication, i.e. it enables the terminal to verify that the MRTD chip is genuine but has two advantages over the original protocol:

- Challenge Semantics are prevented because the transcripts produced by this protocol are non-transferable.
- Besides authentication of the MRTD chip this protocol also provides strong session keys.

CAv1 provides implicit authentication of both the MRTD chip itself and the stored data by performing Secure Messaging using the new session keys.

### 3.4.4 Terminal Authentication Protocol (v1)

The Terminal Authentication Protocol is a two-move challenge-response protocol that provides explicit unilateral authentication of the terminal.

This protocol enables the MRTD chip to verify that the terminal is entitled to access sensitive data. As the terminal may access sensitive data afterwards, all further communication MUST be protected appropriately. Terminal Authentication therefore also authenticates an ephemeral public key chosen by the terminal that was used to set up Secure Messaging with Chip Authentication. The MRTD chip MUST bind the terminal's access rights to Secure Messaging established by the authenticated ephemeral public key of the terminal.

### *3.4.5 Other features*

#### 3.4.5.1 Enhanced protection over Sensitive biometric data reading

The access to sensitive biometric data: the fingerprint and iris stored in DG3 and DG4 are protected in accordance with the requirements of the protection profile and specification. Beyond that, the TOE also provides a feature able to ensure a high level of confidentiality when reading these data. The TOE supports a mechanism enforcing to use a minimum cryptographic strength for the confidentiality, integrity and authenticity protection of these sensitive biometric data when being read. This may be useful for issuing authority that do not consider DES algorithm strong enough to ensure a sufficient level of confidentiality. This mechanism allows the TOE to enforce the terminal using a stronger algorithm such as AES 128, or 192 bits, or 256 bits when reading the sensitive biometric data, and deny access to them if this condition is not met (algorithm not strong enough).

#### 3.4.5.2 Key Usage Counter

The TOE supports an optional feature that allows the issuing country to limit the number of times a key may be used in the field, in particular the Chip Authentication key, the BAC key and the generated secure messaging key.

When configured, the corresponding Key Usage Counter is decremented for every operation the key is used and once the counter reaches zero (i.e. key is blocked), the key can no longer be used.

#### 3.4.5.3 CA Key Renewal / Invalidation

When configured, the Chip Authentication key may be renewed or invalidated. This operation is protected by the Administration Agent key.

# 4 Life Cycle

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP_IC].

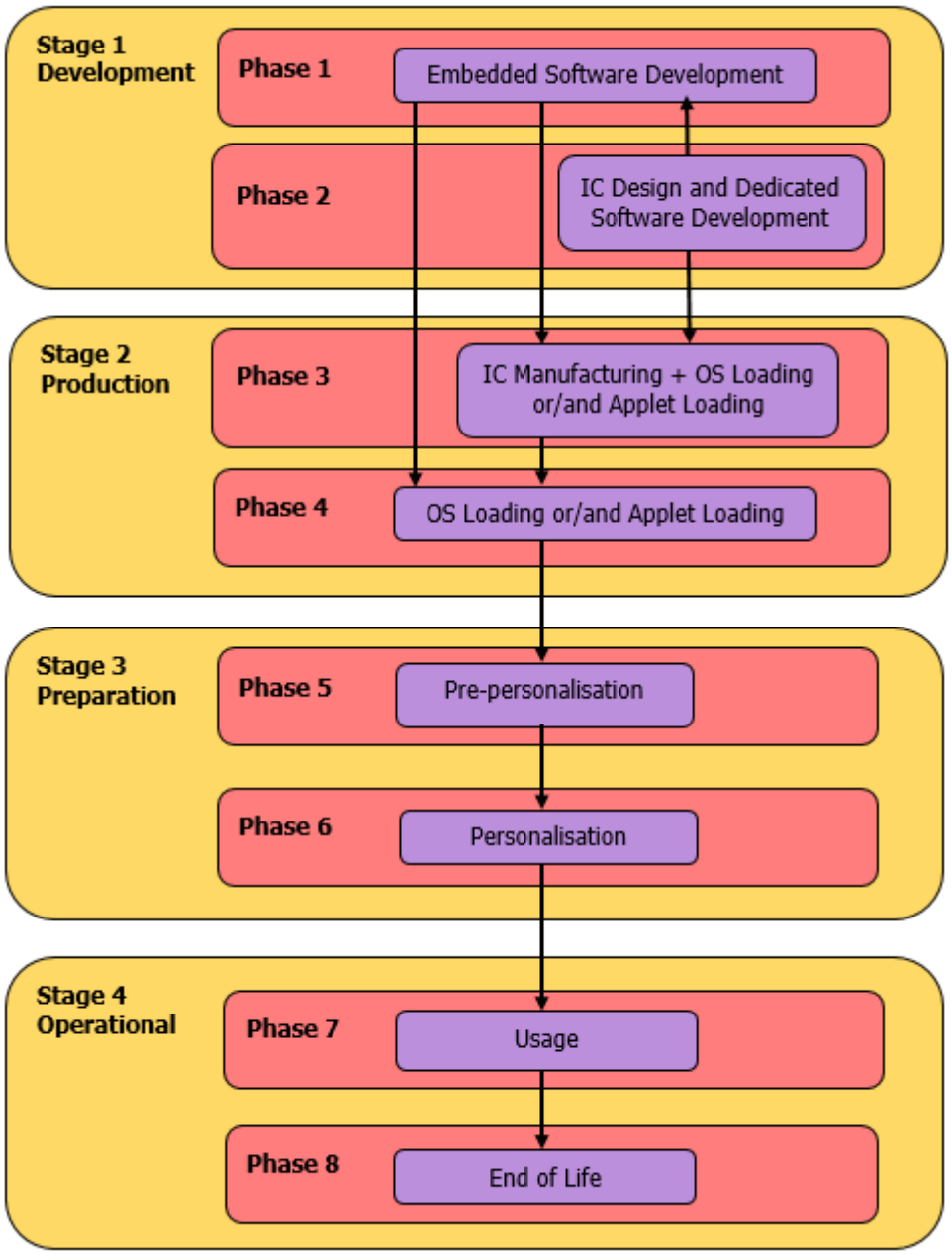



**Figure 2 Life cycle Overview**

## 4.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and CombICAO Applet v3)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification, development and validation of the software (Java Card Open Platform and CombICAO Applet v3).

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.

Roles, actors, sites and coverage for this environment of the product life-cycle are listed in the table below:

| Role | Actor | Site | Covered by |
|---|---|---|---|
| CombICAO Applet v3 Developer | INSI | MANILA and COURBEVOIE R&D sites | ALC |
| Embedded Software Developer (Java Card Open Platform) | IDEMIA | Platform Developer Refer to [ST_PTF] | ALC |
| Redaction and Review of Documents | INSI | MANILA and COURBEVOIE R&D sites | ALC |
| IC Developer | INFINEON | IC Manufacturer Refer to [ST_PTF] | ALC |

**Table 3 : Development R&D Sites**

## 4.2 Production Environment

In this environment, the following two phases take place:

- Phase 3: IC Manufacturing
- Phase 4: ID-One Cosmo X Platform loading and CombICAO Applet v3 loading

The CombICAO Applet v3 run time code is integrated in the FLASH memory of the chip.

Depending on the intention, the following different loading options are supported. Details on delivery methods for each option are provided in the **[AGD_PRE].**

INSI or IDEMIA CC Audited Production Sites are listed below:

| INSI or IDEMIA CC Audited Production Sites/Plants | Country |
|---|---|
| Haarlem | Netherlands |
| Noida | India |
| Ostrava | Czech Republic |
| Shenzhen | China |
| Vitré | France |

**Table 4 : Audited Production Sites**

**(Option 1) Image Loading audited IC Manufacturer site**

FLASH image containing both the "ID-One Cosmo X" Java Card Platform OS along with the CombICAO Applet v3 is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) to the **IC Manufacturer** (Infineon CC Audited Site) to be loaded into FLASH memory. The FLASH image is always encrypted.

**TOE Delivery point (i.e. point in time where the TOE starts to exist):**

- The TOE delivery point occurs in Phase 4, as soon as the loading of the image with ID-One Cosmo X Platform + CombICAO Applet v3 by the IC Manufacturer has been completed.

| Package | Actor for FLASH image loading | Site For FLASH image loading | Covered by CC |
|---|---|---|---|
| FLASH image containing ID-One Cosmo X Platform + CombICAO Applet v3 | IC Manufacturer | IC Manufacturer CC Audited Production Plants specified in [ST_PTF] | ALC |

**Table 5 Option 1: Both Platform and Applet packages are loaded at IC Manufacturer Site**

**(Option 2) Image loading at INSI or IDEMIA and External sites**

FLASH image containing both ID-One Cosmo X Platform along with CombICAO Applet v3 is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) for loading to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

**TOE Delivery point:**

- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Audited INSI or IDEMIA Production Sites, then TOE delivery is considered at the end of Phase 4.

- If loading of ID-One Cosmo X Platform + CombICAO Applet v3 is performed in Non-Audited INSI or IDEMIA Production Sites or External Sites, then TOE delivery is considered after Phase 4.

| Package | Actor for FLASH image loading | Site for FLASH image loading | Covered by CC |
|---|---|---|---|
| FLASH image containing the ID-One Cosmo X Platform + CombICAO Applet v3 | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |

**Table 6 Option 2: Both Platform and Applet packages are loaded at CC Audited Sites**

**(Option 3) Platform loaded by IC Manufacturer, Applet loaded by INSI or 3rd party**
Only the ID-One Cosmo X Platform is delivered to the IC Manufacturer (Infineon Audited Sites) to be loaded.

With the ID-One Cosmo X Platform already loaded (i.e. present) on the chip, the following options (**3a or 3b (i) or 3b (ii) or 3c**) can be chosen for loading the CombICAO Applet v3.

**(Option 3a) Applet loading using GP CLFDB mechanism.**

The CombICAO Applet v3 along with the TOE's guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of the CombICAO Applet v3 on top of the already present ID-One Cosmo X Platform GP Java Card OS in any of these sites is accomplished by using a GP CLFDB decryption Key.

**TOE Delivery points:**

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in a CC Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | IC Manufacturer | IC Manufacturer Production Plants Refer to [PTF-CERT] | ALC |
| CombICAO Applet v3 loaded through GP mechanism using CLFDB Key | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |

**Table 7 Option 3(a): Platform package is loaded at IC Manufacturer Site and Applet package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites through GP Mechanism**

**(Option 3b) Applet loading using the Resident Application**

(i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

CombICAO Applet v3 package is securely loaded via LSK on top of the present ID-One Cosmo X Platform Java Card OS in any of these sites. This loading is accomplished by using the "Resident Application" of the ID-One Cosmo X Platform.

(ii) The DUMP package (including CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by IC Manufacturer (Infineon).

**TOE Delivery points:**

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery after Phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | IC Manufacturer | IC Manufacturer Production Plants Refer to [PTF-CERT] | ALC |
| **3b (i)** CombICAO Applet v3 loaded through Resident Application using LSK format | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |
| **3b (ii)** DUMP PACKAGE Ciphered format [DSK Secret Live Key] | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |

**Table 8 Platform package is loaded at IC Manufacturer Site and Applet package is loaded through resident application using LSK format or DUMP Package in Ciphered format is loaded**

**(Option 3c) Applet loading in plain (unprotected) format using GP**

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision for loading the applet in plain format in **Common Criteria Audited INSI Sites only,** on top of the platform already loaded by IC Manufacturer (Infineon). This applet loading in plain format is not allowed in Non-Audited INSI or IDEMIA Sites or External Sites.

**TOE Delivery points:**

- The loading of CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform is done in plain (unprotected) format in Common Criteria Audited INSI or IDEMIA Production Sites. The TOE delivery is considered at the end of Phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | IC Manufacturer | IC Manufacturer Production Plants Refer to [PTF-CERT] | ALC |
| CombICAO Applet v3 in Plain Format | INSI Authorized Entity | Refer Audited Production Sites Table | ALC |

**Table 9 Option 3(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at Audited INSI Sites only**

**(Option 4) Platform and Applet loaded by INSI or IDEMIA or 3rd party**
Only ID-One Cosmo X Platform is securely delivered directly from the software developer (INSI or IDEMIA R&D Audited Site) for loading to **CC Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

*Note: Here, when the ID-One Cosmo X Platform package is loaded in Non-Audited INSI or IDEMIA Sites or External Sites, then the Platform is in self-protected mode by its secure functions*

The following options (**4a or 4b (i) or 4b (ii) or 4c**) can be chosen for loading applets on top of the already loaded platform.

**(Option 4a) Applet loading using GP CLFDB mechanism**
CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of Applet in any of these sites is done through GP mechanism using CLFDB Key on top of the platform already loaded by **CC Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

**TOE Delivery points:**

- If loading of the CombICAO Applet v3 on top of already loaded ID-One Cosmo X Platform (as described below) is done in CC Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of the CombICAO Applet v3 onto the already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |
| CombICAO Applet v3 loaded through GP mechanism using CLFDB Key | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |

**Table 10 Option 4(a): Platform package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites and Applet package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites through GP Mechanism**

**(Option 4b) Applet loading using the Resident Application**

(i) CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Secure loading of CombICAO Applet v3 is done via LSK on top of the present Cosmo X Java Card OS (already loaded by **Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites)** in any of these sites. This loading is accomplished by using the INSI or IDEMIA "Resident Application" of the ID-One Cosmo X Platform OS

(ii) DUMP package (including the CombICAO Applet v3) with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table) or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

Loading of DUMP PACKAGES in any of these sites is done through Resident Application using DSK secret production key on top of the platform already loaded by **Audited INSI or IDEMIA Production Sites** or **Non-Audited INSI or IDEMIA Sites** or **External Sites**.

**TOE Delivery points:**

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Audited INSI or IDEMIA Production Sites then, TOE delivery is considered at the end of Phase 4.

- If loading of Applet package /DUMP Package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Non-Audited INSI or IDEMIA Production Sites or External Sites then, TOE delivery is considered after Phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |
| **4b (i)** CombICAO Applet v3 package loaded through Resident Application using LSK format | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |
| **4b (ii)** DUMP PACKAGE Ciphered format [DSK Secret Live Key] | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |

**Table 11 Platform package is loaded at Audited INSI or IDEMIA Sites or Non-Audited INSI or IDEMIA Sites or External Sites and Options and Applet package is loaded through Resident application using LSK format or DUMP Package in Ciphered format is loaded**

**(Option 4c) Applet loading in plain (unprotected) format using GP**

CombICAO Applet v3 along with the guidance documentation is securely delivered directly from the Software Developer (INSI or IDEMIA R&D Audited Site) to **Audited INSI or IDEMIA Production Sites** (Refer Audited Production Sites Table).

Here, there is a provision of loading the applet in plain format in Audited INSI or IDEMIA Sites **only,** on top of the platform already loaded by Audited INSI or IDEMIA Production Sites or Non-Audited INSI or IDEMIA Sites or External Sites. This applet loading in plain format is not allowed in Non-Audited INSI or IDEMIA Sites or External Sites.

**TOE Delivery points:**

- Here, since the loading of Applet package on top of already loaded ID-One Cosmo X Platform (as described below) is done in Plain format in CC Audited INSI or IDEMIA Production Sites, so TOE delivery is considered at the end of Phase 4.

| Package | Actor | Site | Covered by |
|---|---|---|---|
| Image containing only ID-One Cosmo X Platform | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |
| | External Authorized Agent | Non-Audited INSI or IDEMIA Sites or External Sites | AGD |
| CombICAO Applet v3 in Plain Format | INSI or IDEMIA Authorized Entity | Refer Audited Production Sites Table | ALC |

**Table 12 Option 4(c): Platform package is loaded at IC Manufacturer Site and Applet package in plain format is loaded at CC Audited INSI Sites only**

## 4.3 Preparation Environment

In this environment, the following two phases take place:

- Phase 5: Pre-personalisation of the applet
- Phase 6: Personalisation

The preparation environment may not necessarily take place in a manufacturing site, but may be performed anywhere. All along these two phases, the TOE is self-protected as it requires the authentication of the pre-personalisation agent or personalisation agent prior to any operation.

The CombICAO Applet v3 is pre-personalised and personalised according to [AGD_PRE].

These two phases are covered by [AGD_PRE] tasks of the TOE and Guidance tasks of [ST_PTF].

## 4.4 Operational Environment

Phase 7: Use Phase

The TOE is used as a travel document's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified for eMRTD application.
Note that applications can be loaded onto the ID-One Cosmo X platform during this phase.

During this phase, the TOE may be used as described in [AGD_OPE] of the TOE.

This phase is covered by [AGD_OPE] tasks of the TOE and Guidance tasks of [ST_PTF].

# 5 Conformance claims

## 5.1 Common Criteria Conformance Claim

This security target claims conformance to the Common Criteria version 3.1, revision 5 [CC2] and [CC3].

The conformance to the CC is claimed as follows:

| CC | Conformance rationale |
|---|---|
| Part 2 | Conformance with the extended[3] part:<br>▪ FAU_SAS.1 "Audit Storage"<br>▪ FCS_RND.1 "Quality metric for random numbers"<br>▪ FMT_LIM.1 "Limited capabilities"<br>▪ FMT_LIM.2 "Limited availability"<br>▪ FPT_EMS.1 "TOE Emanation"<br>▪ FIA_API.1 "Authentication Proof of Identity" |
| Part 3 | Conformance to EAL 5, augmented with<br>▪ AVA_VAN.5: "Advanced methodical vulnerability analysis"<br>▪ ALC_DVS.2: "Sufficiency of security measures"<br>▪ ALC_FLR.1: "Basic flaw remediation |

**Table 13 Common Criteria conformance claim**

The Common Methodology for Information Technology Security Evaluation [CEM] has been taken into account.

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this ST as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP_BAC]. Due to the fact that [PP_BAC] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately.

There are separate Security Targets for BAC and EAC. Note, that the claim for conformance to the BAC-PP [PP_BAC] does not require the conformance claim to [PP_EAC]. Nevertheless claiming conformance of [PP_EAC] requires that the TOE meets a (separate) ST conforming to the BAC-PP [PP_BAC].

[3] The rationale for SFR addition is described in the relative PP

## 5.2 Protection Profile Conformance Claim

This security target (ST) claims strict conformance to:

- [PP_EAC] : Common Criteria Protection Profile Machine readable travel documents with "ICAO Application", Extended Access control – BSI-PP-0056 v1.10 25th march 2009.

This ST also addresses Active Authentication as an additional authentication protocol.
Since the Chip Authentication protocol is an alternative to the Active Authentication defined in [ICO_9303], the additional assumptions and security objectives for the operational environment counter the same threats as the ones for chip authentication. They however do not mitigate the threat, and instead provide an additional functionality to the ones defined in the PP.

## 5.3 Package Claim

This ST is conforming to assurance package EAL5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5 defined in CC part 3 [CC3].

### *5.3.1 Main aspects*

- The TOE description is based on the TOE definition and TOE usage of [PP_EAC]. It was enhanced by product specific details.

- All definitions of the security problem definition in [PP_EAC] have been taken exactly from the protection profile in the same wording.

- All security objectives have been taken exactly from [PP_EAC] in the same wording.

- The part of extended components definition has been taken originally from [PP_EAC].

- All SFRs for the TOE have been taken originally from the [PP_EAC] added by according iterations, selections and assignments.

- The security assurance requirements (SARs) have been taken originally from the [PP_EAC]. The requirements are shifted to those of EAL 5+.

### *5.3.2 Overview of differences between the PP and the ST*

The following parts list additional Subject, Threats and Objectives for this TOE, which are not in [PP_EAC].

These additions do not contradict with any other Subjects, Threats and Objectives of the TOE of the original PP nor mitigate a threat (or part of a threat), meant to be addressed by security objectives for the TOE in the PP.

### 5.3.3 Additional Subjects

The following additional Subject is identified:

- **Administrator**

### 5.3.4 Additional Threats

The following additional Threats are identified:

- **T.Configuration**
- **T. Forgery_Supplemental_Data**
- **T.ADMIN_Configuration**
- **T.Key_Access**

### 5.3.5 Additional Organisational Security Policies

The following additional Organisational Security Policy is identified:

- **P.Activ_Auth**

### 5.3.6 Additional Security Objectives

The following additional Security Objectives of the TOE are identified:

- **OT.Configuration**
- **OT.Update_File**
- **OT.AC_SM_Level**
- **OT.AA_Proof**
- **OT.Data_Int_AA**
- **OT.ADMIN_Configuration**
- **OT.Key_Usage_Counter**

### 5.3.7 Additional Security Objectives for the Operational Environment

The following additional Security Objectives of the Operational Environment are identified:

- **OE.Exam_MRTD_AA**
- **OE.Prot_Logical_MRTD_AA**
- **OE.Activ_Auth_Verif**
- **OE.Activ_Auth_Sign**

### 5.3.8 Additional Security Functional Requirements

The following additional Security Functional Requirements are identified:

- **FCS_CKM.1/CA_DATA_GEN**
- **FCS_CKM.1/GP**
- **FCS_CKM.1/GP_ENC**
- **FCS_CKM.1/GP_AUTH**
- **FCS_CKM.1/GP_MAC**
- **FCS_CKM.1/GP_KEY_DEC**
- **FCS_CKM.1/AA**
- **FIA_UID.1/MP**
- **FIA_UAU.1/MP**
- **FIA_UAU.6/MP**

- **FIA_AFL.1/MP**
- **FDP_ACC.1/UPD_FILE**
- **FDP_ACF.1/UPD_FILE**
- **FDP_DAU.1/AA**
- **FDP_ITC.1/AA**
- **FMT_MOF.1/AA**
- **FMT_MOF.1/GP**
- **FMT_MTD.1/LCS_PERS**
- **FMT_MTD.1/UPD_FILE**
- **FMT_MTD.1/SM_LVL_DG3_DG4**
- **FMT_MTD.1/SM_LVL**
- **FMT_MTD.1/AA_KEY_READ**
- **FMT_MTD.1/AA_KEY_WRITE**
- **FMT_MTD.1/ADMIN**
- **FMT_MTD.1/Key_Usage_Counter**
- **FTP_ITC.1/MP**

## 5.4 CC Conformance and usage in real life

In the real life, for interoperability purposes, the MRTD will most likely support BAC, PACE and EAC.

- If the terminal reads MRTD data by performing only BAC, the security of the MRTD will be covered by the security evaluation of the TOE described in the ST claiming compliance to the [PP_BAC] only.

- If the terminal reads the content of the MRTD by performing BAC then EAC, the security of the MRTD will be covered by the security evaluation of (1) the TOE described by the ST claiming compliance to [PP_BAC] and (2) the TOE described by the ST claiming compliance to [PP_EAC], assuming PACE is not supported by the terminal (as not used for the inspection procedure)

- If the terminal reads the content of the MRTD by performing PACE then EAC, the security of the MRTD will be covered by the security evaluation of the TOE described by the ST claiming compliance to [PP_EACwPACE], assuming PACE is supported by the terminal (as not used for the inspection procedure).

# 6 Security Problem Definition

## 6.1 Assets

**Logical MRTD sensitive User Data**

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

*Application Note:*

Due to interoperability reasons the 'ICAO Doc 9303' [ICAO_9303] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [PP_BAC]).

**Authenticity of the MRTD's chip**

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

## 6.2 Users / Subjects

### *6.2.1 Additional Subject*

**Administrator**

The role ADMIN is an Administrator in use phase who can act on the TOE configuration. The administrative actions are dedicated to:

- Manage symmetric authentication using Administration Agent keys,
- Configure the size or value of the Chip Authentication key to be modified in USE phase,
- Change the key parameters during the key generation process,
- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key.

### *6.2.2 Miscellaneous*

**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.

**Personalization Agent**

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris

image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [ICAO_9303].

**Country Verifying Certification Authority**

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

**Document Verifier**

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

**Terminal**

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

**Inspection system (IS)**

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System (BIS) (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism and (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the MRTD or other parts of the passport book providing this information. The General Inspection System (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism. The Extended Inspection System (EIS) in addition to the General Inspection System (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined of the Inspection System Certificates.

**MRTD Holder**

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

**Traveler**

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

**Attacker**

A threat agent trying (i) to manipulate the logical MRTD without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4) or (iii) to forge a genuine MRTD.

*Application Note:*

Note that an attacker trying to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD) is not considered by this ST since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [PP_BAC]. The same holds for the confidentiality of the user data EF.DG1, EF.DG2, EF.DG5 to EF.DG16 as well as EF.SOD and EF.COM.

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

## 6.3 Threats

### *6.3.1 Threats from Protection Profile*

**T.Read_Sensitive_Data**

*Adverse action*: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP_BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

*Threat agent*: having high attack potential, knowing the Document Basic Access Keys, being in possession of a legitimate MRTD

*Asset*: confidentiality of sensitive logical MRTD (i.e. biometric reference) data,

**T.Forgery**

*Adverse action*: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged

to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

*Threat agent*: having high attack potential, being in possession of one or more legitimate MRTDs

*Asset*: authenticity of logical MRTD data,

**T.Counterfeit**

*Adverse action*: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD. The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

*Threat agent*: having high attack potential, being in possession of one or more legitimate MRTDs

*Asset*: authenticity of logical MRTD data,

**T.Abuse-Func**

*Adverse action*: An attacker may use functions of the TOE which shall not be used in "Operational Use" 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.

*Threat agent*: having high attack potential, being in possession of a legitimate MRTD

*Asset*: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

**T.Information_Leakage**

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

*Threat agent*: having high attack potential, being in possession of a legitimate MRTD

*Asset*: confidentiality of logical MRTD and TSF data

**T.Phys-Tamper**

*Adverse action*: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features

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

*Threat agent*: having high attack potential, being in possession of a legitimate MRTD

*Asset*: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

**T.Malfunction**

*Adverse action*: An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

*Threat agent*: having high attack potential, being in possession of a legitimate MRTD

*Asset*: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

### *6.3.2 Additional Threats Identified*

**T.Configuration**

*Adverse action*: An attacker may access to the TOE at Manufacturing and Personalization phases (steps 5 and 6) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

*Threat agent*: having high attack potential, being in possession of one or more MRTD in Pre-personalization or Personalization phases.

*Asset*: authenticity of logical MRTD data

**T. Forgery_Supplemental_Data**

*Adverse action*: An attacker alters fraudulently the data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object. This may lead the extended inspection system (EIS) using these data to be deceived.

*Threat agent*: having high attack potential, being in possession of one or more legitimate MRTDs.

*Asset*: authenticity of data stored in files other than EF.DG1 to EF.DG16, EF.COM and EF document security object

**T.ADMIN_Configuration**

*Adverse action*: An attacker may access to the TOE at user phase (phase 7) to try to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the eDigitalIdentity document's embedded software.

*Threat agent*: having high attack potential, being in possession of one or more legitimate eDigitalIdentity document in Operational use phase.

*Asset*: authenticity of logical eDigitalIdentity document data.

**T.Key_Access**

*Adverse action*: An attacker may access to the internal secret cryptographic keys of the TOE.

*Threat agent*: having high attack potential, knowing the key values, being in possession of a legitimate eDigitalIdentity document.

*Asset*: TOE internal secret cryptographic keys

## 6.4 Organisational Security Policies

### *6.4.1 OSP's from Protection Profile*

**P.BAC-PP**

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the [ICAO_9303] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP_BAC] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

*Application Note:*

The organizational security policy P.Personal_Data drawn from the 'ICAO Doc 9303' [ICAO_9303] is addressed by the [PP-BAC] (cf. P.BAC-PP). The confidentiality of the personal data other than EF.DG3 and EF.DG4 is ensured by the BAC mechanism. Note the BAC mechanisms may not resist attacks with high attack potential (cf. [PP-BAC]). The TOE shall protect the sensitive biometric reference data in EF.DG3 and EF.DG4 against attacks with high attack potential. Due to the different resistance the protection of EF.DG3 and EF.DG4 on one side and the other EF.SOD, EF.COM, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 are addressed separated protection profiles, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates (cf. also to application note 1).

**P.Sensitive_Data**

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

sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication.

**P.Manufact**

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

**P.Personalization**

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

### *6.4.2 Additional OSP*

**P.Activ_Auth**

The terminal implements the Active Authentication protocol as described in [ICAO_9303]

## 6.5 Assumptions

**A.MRTD_Manufact**

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

**A.MRTD_Delivery**

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

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

**A.Pers_Agent**

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

**A.Insp_Sys**

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 Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303]. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD. The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

**A.Signature_PKI**

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

**A.Auth_PKI**

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

**A.Insp_Sys_AA**

The Inspection System implements the Active Authentication Mechanism. The Inspection System verifies the authenticity of the MRTD's chip during inspection using the signature returned by the TOE during Active Authentication.

# 7 Security Objectives

## 7.1 Security Objectives for the TOE

### *7.1.1 Security Objectives from Protection Profile*

**OT.AC_Pers**

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO_9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG3 to EF.DG16 are added.

*Application Note:*

The OT.AC_Pers implies that

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

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

**OT.Data_Int**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

**OT.Sens_Data_Conf**

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

**OT.Identification**

The TOE must provide means to store IC Identification and Pre-Personalization Data in its nonvolatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre- Personalization data includes writing of the Personalization Agent Key(s).

**OT.Chip_Auth_Proof**

The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [TR_03110-3]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

*Application Note:*

The OT.Chip_Auth_Proof implies the MRTD's chip to have (i) a unique identity as given by the MRTD's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of MRTD's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the MRTD's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS [ICAO_9303] and (ii) the hash value of the Chip Authentication Public Key in the Document Security Object signed by the Document Signer.

**OT.Prot_Abuse-Func**

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to (i) disclose critical User Data, (ii) manipulate critical User Data of the IC Embedded Software, (iii) manipulate Soft-coded IC Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

**OT.Prot_Inf_Leak**

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

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

*Application Note:*

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

**OT.Prot_Phys-Tamper**

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

**OT.Prot_Malfunction**

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

*Application Note:*

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

### *7.1.2 Additional Security Objectives Identified*

**OT.Configuration**

During Pre-personalization and Personalization phases, the TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. It must also ensure secure erasing of useless keys.

**OT.Update_File**

During Operational Use phase, the TOE must allow the modification of Updatable Data if the write access to these objects is fulfilled by the Terminal.

**OT.AC_SM_Level**

During Operational Use phase, the TOE must allow read access to sensitive biometric data only if the Secure Messaging level reaches or exceeds the one specified in the biometric data Access Conditions data object.

**OT.AA_Proof**

The TOE must support the Inspection Systems to verify the identity and authenticity of MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO_9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

**OT.Data_Int_AA**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the

logical MRTD data during their transmission to the General Inspection System after Active Authentication.

**OT.ADMIN_Configuration**

***Protection of the TOE administration***

In user phase, the TOE must ensure the administration actions are only authorized for Administrator. The TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions.

**OT.Key_Usage_Counter**

***Configuration of Key Usage Counter***

The TOE must protect the key usage through OT.Key_Usage_Counter that support a Key Usage Counter which should be decremented by one each time the key is used. Once the counter is depleted, the key should become unusable.

## 7.2 Security Objectives for the Operational Environment

### *7.2.1 Security Objectives for the Operational Environment from Protection Profile*

#### 7.2.1.1 Issuing State or Organization

**OE.MRTD_Manufact**

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

**OE.MRTD_ Delivery**

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

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

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process. Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the

procedure requirements and be able to act fully in accordance with the above expectations.

**OE.Personalization**

The issuing State or Organization must ensure that the Personalization Agents acting on behalf of the issuing State or Organization (i) establish the correct identity of the holder and create biographical data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

**OE.Pass_Auth_Sign**

The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity. The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO_9303].

**OE.Auth_Key_MRTD**

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

**OE.Authoriz_Sens_Data**

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

**OE.BAC_PP**

It has to be ensured by the issuing State or Organization, that the TOE is additionally successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP_BAC]. This is necessary to cover the BAC mechanism ensuring the confidentiality of standard user data and preventing the traceability of the MRTD data. Note that due to the differences within the assumed attack potential the addressed evaluation and certification is a technically separated process.

#### 7.2.1.2 Receiving State or Organization

**OE.Exam_MRTD**

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [ICAO_9303]. Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

**OE.Passive_Auth_Verif**

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

**OE.Prot_Logical_MRTD**

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

*Application Note:*

[TR_03110-3] supposes that the GIS and the EIS follow the order (i) running the Basic Access Control Protocol, (ii) reading and verifying only those parts of the logical MRTD that are necessary to know for the Chip Authentication Mechanism (i.e. Document Security Object and Chip Authentication Public Key), (iii) running the Chip Authentication Protocol, and (iv) reading and verifying the less-sensitive data of the logical MRTD after Chip Authentication. The supposed sequence has the advantage that the less-sensitive data are protected by secure messaging with cryptographic keys based on the Chip Authentication Protocol which quality is under control of the TOE. The inspection system will prevent additionally eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol. Note that reading the lesssensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this ST. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

**OE.Ext_Insp_Systems**

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

### *7.2.2 Additional Security Objectives Identified for the Operational Environment*

**OE.Exam_MRTD_AA**

Aditionally to the OE.Exam_MRTD, the inspection systems perform the Active Authentication protocol to verify the Authenticity of the presented MRTD's chip.

**OE.Prot_Logical_MRTD_AA**

Aditionally to the OE.Prot_Logical_MRTD, the inspection system prevents eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Active Authentication Protocol.

**OE.Activ_Auth_Verif**

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

**OE.Activ_Auth_Sign**

The issuing State or Organization has to establish the necessary public key infrastructure in order to (i) generate the MRTD's Active Authentication Key Pair, (ii) ensure the secrecy of the MRTD's Active Authentication Private Key, sign and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 and (iii) support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Active Authentication Public Key by means of the Document Security Object.

## 7.3 Security Objectives Rationale

### *7.3.1 Threats*

#### 7.3.1.1 Threats from Protection Profile

**T.Read_Sensitive_Data** The threat T.Read_Sensitive_Data "Read the sensitive biometric reference data" is countered by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by OE.Authoriz_Sens_Data "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

This threat is also covered by OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" that enhences this protection by allowing the issuing State or Organization to require the usage of a secure messaging with a minimum security level for accessing the sensitive biometric reference data. The strength of the secure messaging is tightly bound to the underlying block Cipher involved (DES, AES-

128/192/256). This objective allows an issuing State or Organization to set a secure messaging level it considers as sufficient to ensure a long term confidentiality of the sensitive biometric data of its citizen when being read.

**T.Forgery** The threat T.Forgery "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent. 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" and OE.Exam_MRTD_AA shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to OE.Pass_Auth_Sign "Authentication of logical MRTD by Signature" and verified by the inspection system according to OE.Passive_Auth_Verif "Verification by Passive Authentication".

**T.Counterfeit** The threat T.Counterfeit "MRTD's chip" addresses the attack of unauthorized copy or reproduction of the genuine MRTD chip. This attack is thwarted by chip an identification and authenticity proof required by OT.Chip_Auth_Proof "Proof of MRTD's chip authentication" using a authentication key pair to be generated by the issuing State or Organization. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by OE.Auth_Key_MRTD "MRTD Authentication Key".

This attack is also thwarted by Active Authentication proving the authenticity of the chip as required by OT.AA_Proof and OT.Data_Int_AA using a authentication key pair to be generated by the issuing State or Organization.

According to OE.Exam_MRTD "Examination of the MRTD passport book" the General Inspection system has to perform the Chip Authentication Protocol to verify the authenticity of the MRTD's chip.

OE.Activ_Auth_Verif and OE.Activ_Auth_Sign covers also this threat enabling the possibility of performing an Active Authentication which reinforce the security associated to the communication.

**T.Abuse-Func** The threat T.Abuse-Func "Abuse of Functionality" addresses attacks of misusing MRTD's functionality to disable or bypass the TSFs. The security objective for the TOE OT.Prot_Abuse-Func "Protection against abuse of functionality" ensures that the usage of functions which may not be used in the "Operational Use" phase is effectively prevented. Therefore attacks intending to abuse functionality in order to disclose or manipulate critical (User) Data or to affect the TOE in such a way that security features or TOE's functions may be bypassed, deactivated, changed or explored shall be effectively countered.

**T.Information_Leakage** The threat T.Information_Leakage "Information Leakage from MRTD's chip", is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the

directly related security objective OT.Prot_Inf_Leak "Protection against Information Leakage".

**T.Phys-Tamper** The threat T.Phys-Tamper "Physical Tampering" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Phys-Tamper "Protection against Physical Tampering".

**T.Malfunction** The threat T.Malfunction "Malfunction due to Environmental Stress" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objective OT.Prot_Malfunction "Protection against Malfunctions".

#### 7.3.1.2 Additional Threats Identified

**T.Configuration** The threat T.Configuration "Tampering attempt of the TOE during preparation" addresses attacks in Pre-personalization and Personalization phases. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Personalization system. Protection of the TOE during these two phases is directly addressed by OT.Configuration "Protection of the TOE preparation".

**T. Forgery_Supplemental_Data** The threat T. Forgery_Supplemental_Data "Forgery of supplemental data stored in the TOE" addresses the fraudulent alteration of Updatable Data. The TOE protects the update of these data thanks to OT.Update_File "Modification of file in Operational Use Phase" that ensures inspection system are authenticated and data to be updated are sent through a secure channel ensuring integrity, authenticity and confidentiality.

**T.ADMIN_Configuration** The threat T.ADMIN_Configuration "Tampering attempt of the TOE during administration" addresses attacks in Operational use phase. The attacker trying to access to unauthorized TOE functions, trying to access or to modify sensitive information exchanged between the TOE and the Administartion system. Protection of the TOE during this phases is directly addressed by OT.ADMIN_Configuration "Protection of the TOE administration".

**T.Key_Access** The threat T.Key_Access addresses the threat of access to the internal secret cryptographic keys of the TOE. The TOE protects the key usage through OT.Key_Usage_Counter "Configuration of Key Usage Counter" that support a Key Usage Counter that is decremented by one each time the key is used. Once the counter is depleted, the key becomes unusable. In the case of CA key, the Key Usage Counter will be reset to the maximum usage if the CA key is re-generated in USE phase.

### *7.3.2 Organisational Security Policies*

#### 7.3.2.1 OSP's from Protection Profile

**P.BAC-PP** The OSP P.BAC-PP is directly addressed by the OE.BAC_PP.

**P.Sensitive_Data** The OSP P.Sensitive_Data "Privacy of sensitive biometric reference data" is fulfilled by the TOE-objective OT.Sens_Data_Conf "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organization as required by OE.Authoriz_Sens_Data "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by OE.Ext_Insp_Systems "Authorization of Extended Inspection Systems".

**P.Manufact** The OSP P.Manufact "Manufacturing of the MRTD's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by OT.Identification.

**P.Personalization** 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 Key(s) according to OT.Identification "Identification and Authentication of the TOE". The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" limits the management of TSF data and management of TSF to the Personalization Agent.

#### 7.3.2.2 Additional OSP

**P.Activ_Auth** The OSP P.Activ_Auth requires the implementation of the Active Authentication protocol as enforced by OT.AA_Proof.

### *7.3.3 Assumptions*

**A.MRTD_Manufact** The assumption A.MRTD_Manufact "MRTD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment OE.MRTD_Manufact "Protection of the MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

**A.MRTD_Delivery** The assumption A.MRTD_ Delivery "MRTD delivery during step 4 to 6" is covered by the security objective for the TOE environment OE.MRTD_ Delivery "Protection of the MRTD delivery" that requires to use security procedures during delivery steps of the MRTD.

**A.Pers_Agent** 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.

**A.Insp_Sys** 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" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment OE.Prot_Logical_MRTD "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

**A.Signature_PKI** The assumption A.Signature_PKI "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment OE.Pass_Auth_Sign "Authentication of logical MRTD by Signature" covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by OE.Exam_MRTD "Examination of the MRTD passport book".

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

**A.Insp_Sys_AA** The examination of the MRTD passport book addressed by the assumption A.Insp_Sys_AA "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment OE.Exam_MRTD_AA "Examination of the MRTD passport book". The security objectives for the TOE environment OE.Prot_Logical_MRTD_AA "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Active Authentication Protocol and to protect the logical MRTD data during the transmission and the internal handling.

### *7.3.4 SPD and Security Objectives*

| Threats | Security Objectives | Rationale |
|---|---|---|
| T.Read_Sensitive_Data | OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems, OT.AC_SM_Level | Section 7.3.1 |
| T.Forgery | OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRTD, OE.Passive_Auth_Verif, OE.Exam_MRTD_AA | Section 7.3.1 |
| T.Counterfeit | OT.Chip_Auth_Proof, OE.Auth_Key_MRTD, OE.Exam_MRTD, OT.AA_Proof, OT.Data_Int_AA, OE.Activ_Auth_Verif, | Section 7.3.1 |

| | | |
|---|---|---|
| | OE.Activ_Auth_Sign | |
| T.Abuse-Func | OT.Prot_Abuse-Func | Section 7.3.1 |
| T.Information_Leakage | OT.Prot_Inf_Leak | Section 7.3.1 |
| T.Phys-Tamper | OT.Prot_Phys-Tamper | Section 7.3.1 |
| T.Malfunction | OT.Prot_Malfunction | Section 7.3.1 |
| T.Configuration | OT.Configuration | Section 7.3.1 |
| T. Forgery_Supplemental_Data | OT.Update_File | Section 7.3.1 |
| T.ADMIN_Configuration | OT.ADMIN_Configuration | Section 7.3.1 |
| T.Key_Access | OT.Key_Usage_Counter | Section 7.3.1 |

**Table 14 Threats and Security Objectives - Coverage**

| Security Objectives | Threats |
|---|---|
| OT.AC_Pers | T.Forgery |
| OT.Data_Int | T.Forgery |
| OT.Sens_Data_Conf | T.Read_Sensitive_Data |
| OT.Identification | |
| OT.Chip_Auth_Proof | T.Counterfeit |
| OT.Prot_Abuse-Func | T.Abuse-Func |
| OT.Prot_Inf_Leak | T.Information_Leakage |
| OT.Prot_Phys-Tamper | T.Forgery, T.Phys-Tamper |
| OT.Prot_Malfunction | T.Malfunction |
| OT.Configuration | T.Configuration |
| OT.Update_File | T. Forgery_Supplemental_Data |
| OT.AC_SM_Level | T.Read_Sensitive_Data |
| OT.AA_Proof | T.Counterfeit |
| OT.Data_Int_AA | T.Counterfeit |
| OT.ADMIN_Configuration | T.ADMIN_Configuration |
| OT.Key_Usage_Counter | T.Key_Access |
| OE.MRTD_Manufact | |
| OE.MRTD_ Delivery | |
| OE.Personalization | |
| OE.Pass_Auth_Sign | T.Forgery |
| OE.Auth_Key_MRTD | T.Counterfeit |
| OE.Authoriz_Sens_Data | T.Read_Sensitive_Data |

| | |
|---|---|
| OE.BAC_PP | |
| OE.Exam_MRTD | T.Forgery, T.Counterfeit |
| OE.Passive_Auth_Verif | T.Forgery |
| OE.Prot_Logical_MRTD | |
| OE.Ext_Insp_Systems | T.Read_Sensitive_Data |
| OE.Exam_MRTD_AA | T.Forgery |
| OE.Prot_Logical_MRTD_AA | |
| OE.Activ_Auth_Verif | T.Counterfeit |
| OE.Activ_Auth_Sign | T.Counterfeit |

**Table 15 Security Objectives and Threats - Coverage**

| Organisational Security Policies | Security Objectives | Rationale |
|---|---|---|
| P.BAC-PP | OE.BAC_PP | Section 7.3.2 |
| P.Sensitive_Data | OT.Sens_Data_Conf, OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems | Section 7.3.2 |
| P.Manufact | OT.Identification | Section 7.3.2 |
| P.Personalization | OT.AC_Pers, OT.Identification, OE.Personalization | Section 7.3.2 |
| P.Activ_Auth | OT.AA_Proof | Section 7.3.2 |

**Table 16 OSPs and Security Objectives - Coverage**

| Security Objectives | Organisational Security Policies |
|---|---|
| OT.AC_Pers | P.Personalization |
| OT.Data_Int | |
| OT.Sens_Data_Conf | P.Sensitive_Data |
| OT.Identification | P.Manufact, P.Personalization |
| OT.Chip_Auth_Proof | |
| OT.Prot_Abuse-Func | |
| OT.Prot_Inf_Leak | |
| OT.Prot_Phys-Tamper | |
| OT.Prot_Malfunction | |
| OT.Configuration | |
| OT.Update_File | |
| OT.AC_SM_Level | |
| OT.AA_Proof | P.Activ_Auth |

| | |
|---|---|
| OT.Data_Int_AA | |
| OT.ADMIN_Configuration | |
| OT.Key_Usage_Counter | |
| OE.MRTD_Manufact | |
| OE.MRTD_Delivery | |
| OE.Personalization | P.Personalization |
| OE.Pass_Auth_Sign | |
| OE.Auth_Key_MRTD | |
| OE.Authoriz_Sens_Data | P.Sensitive_Data |
| OE.BAC_PP | P.BAC-PP |
| OE.Exam_MRTD | |
| OE.Passive_Auth_Verif | |
| OE.Prot_Logical_MRTD | |
| OE.Ext_Insp_Systems | P.Sensitive_Data |
| OE.Exam_MRTD_AA | |
| OE.Prot_Logical_MRTD_AA | |
| OE.Activ_Auth_Verif | |
| OE.Activ_Auth_Sign | |

**Table 17 Security Objectives and OSPs - Coverage**

| Assumptions | Security Objectives for the Operational Environment | Rationale |
|---|---|---|
| A.MRTD_Manufact | OE.MRTD_Manufact | Section 7.3.3 |
| A.MRTD_Delivery | OE.MRTD_Delivery | Section 7.3.3 |
| A.Pers_Agent | OE.Personalization | Section 7.3.3 |
| A.Insp_Sys | OE.Exam_MRTD, OE.Prot_Logical_MRTD | Section 7.3.3 |
| A.Signature_PKI | OE.Pass_Auth_Sign, OE.Exam_MRTD | Section 7.3.3 |
| A.Auth_PKI | OE.Authoriz_Sens_Data, OE.Ext_Insp_Systems | Section 7.3.3 |
| A.Insp_Sys_AA | OE.Exam_MRTD_AA, OE.Prot_Logical_MRTD_AA | Section 7.3.3 |

**Table 18 Assumptions and Security Objectives for the Operational Environment - Coverage**

| Security Objectives for the Operational Environment | Assumptions |
|---|---|
| OE.MRTD_Manufact | A.MRTD_Manufact |
| OE.MRTD_Delivery | A.MRTD_Delivery |

| | |
|---|---|
| OE.Personalization | A.Pers_Agent |
| OE.Pass_Auth_Sign | A.Signature_PKI |
| OE.Auth_Key_MRTD | |
| OE.Authoriz_Sens_Data | A.Auth_PKI |
| OE.BAC_PP | |
| OE.Exam_MRTD | A.Insp_Sys, A.Signature_PKI |
| OE.Passive_Auth_Verif | |
| OE.Prot_Logical_MRTD | A.Insp_Sys |
| OE.Ext_Insp_Systems | A.Auth_PKI |
| OE.Exam_MRTD_AA | A.Insp_Sys_AA |
| OE.Prot_Logical_MRTD_AA | A.Insp_Sys_AA |
| OE.Activ_Auth_Verif | |
| OE.Activ_Auth_Sign | |

**Table 19 Security Objectives for the Operational Environment and Assumptions - Coverage**

# 8 Extended Requirements

## 8.1 Extended Families

### *8.1.1 Extended Family FPT_EMS - TOE Emanation*

#### 8.1.1.1 Description

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE?s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

#### 8.1.1.2 Extended Components

**Extended Component FPT_EMS.1**

Family behavior:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

| **FPT_EMS TOE Emanation** | 1 |
|---|---|

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if **FAU_GEN** (*Security audit data generation*) isincluded in a PP or ST using FPT_EMS.1.

*Definition*

| **FPT_EMS.1 TOE Emanation** |
|---|

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

### *8.1.2 Extended Family FMT_LIM - Limited capabilities*

#### 8.1.2.1 Description

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

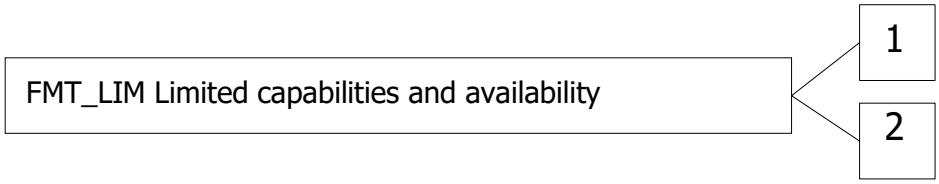
#### 8.1.2.2 Extended Components

**Extended Component FMT_LIM.1**

Family behavior:

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

Component levelling:




FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuinepurpose.

| | |
|---|---|
| FMT_LIM.2 | Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle. |
| Management: | FMT_LIM.1, FMT_LIM.2<br>There are no management activities foreseen. |
| Audit: | FMT_LIM.1, FMT_LIM.2<br>There are no actions defined to be auditable. |

*Definition*

**FMT_LIM.1 Limited capabilities**

**FMT_LIM.1.1** The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT_LIM.2 Limited availability.

**Extended Component FMT_LIM.2**

*Definition*

**FMT_LIM.2 Limited availability**

**FMT_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: Limited capability and availability policy]

Hierarchical to: No other components

Dependencies: FMT_LIM.1 Limited availability.

### *8.1.3 Extended Family FIA_API - Authentication Proof of Identity*

#### 8.1.3.1 Description

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

**Application note 10:** The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Explicitly stated IT security requirements (APE_SRE)') from a TOE point of view.

#### 8.1.3.2 Extended Components

**Extended Component FIA_API.1**

Family behavior:

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

Component levelling:

| FIA_API Authentication Proof of Identity | 1 |
|---|---|

Management FIA_API.1

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

Audit: FIA_API.1
There are no actions defined to be auditable.

*Definition*

**FIA_API.1 Authentication Proof of Identity**

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

Hierarchical to: No other components

Dependencies: No dependencies.

### *8.1.4 Extended Family FAU_SAS - Audit data storage*

#### 8.1.4.1 Description

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

The family 'Audit data storage (FAU_SAS)' is specified as follows:
**FAU_SAS Audit data storage**

Family behavior

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

Component levelling


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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

**FAU_SAS.1 Audit storage**

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

Hierarchical to: No other components

Dependencies: No Depenedencies

### *8.1.5 Extended Family FCS_RND - Generation of random numbers*

#### 8.1.5.1 Description

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

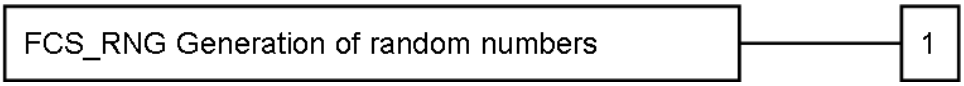
#### 8.1.5.2 Extended Components

**Extended Component FCS_RND.1**

Family behavior:

This family defines requirements for the generation random number where the random numbers are intended to be used for cryptographic purposes.

Component levelling:



Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

*Definition*

**FCS_RND.1 Quality metric for random numbers**

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

Hierarchical to: No other components.

Dependencies: No dependencies.

# 9 Security Requirements

## 9.1 Security Functional Requirements

### *9.1.1 Class FAU Security Audit*

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

**FAU_SAS.1 Audit storage**

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

### *9.1.2 Class FCS Cryptographic Support*

**FCS_CKM.1/CA Cryptographic key generation**

**FCS_CKM.1.1/CA** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **based on ECDH compliant to [ISO11770-3]** and specified cryptographic key sizes **192 to 512 bit** that meet the following: **[TR-03110-3]**.

*Application Note:*

ISO-15946 defined in the protection profile has been replaced since Part 3 that dealt with Key Management using Elliptic Curve has been withdrawn and instead revised by [ISO11770-3].

**FCS_CKM.4 Cryptographic key destruction**

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroisation** that meets the following: **none**.

**FCS_COP.1/SHA Cryptographic operation**

**FCS_COP.1.1/SHA** The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512** and cryptographic key sizes **none** that meet the following: **[FIPS_180_4]**.

## FCS_COP.1/SYM Cryptographic operation

**FCS_COP.1.1/SYM** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

| Cryptographic Operations | Algorithms | Key sizes | Norms |
|---|---|---|---|
| secure messaging-encryption and decryption | AES in CBC mode | 128, 192 and 256 bits | [TR-03110-3] |
| secure messaging-encryption and decryption | TDES in CBC mode | 112 bits | [TR-03110-3] |

## FCS_COP.1/MAC Cryptographic operation

**FCS_COP.1.1/MAC** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

| Cryptographic Operations | Algorithms | Key sizes | Standard |
|---|---|---|---|
| secure messaging - message authentication code | AES CMAC | 128, 192 and 256 bits | [TR-03110-3] |
| secure messaging - message authentication code | Retail MAC | 112 bits | [TR-03110-3] |

## FCS_COP.1/SIG_VER Cryptographic operation

**FCS_COP.1.1/SIG_VER** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

| Cryptographic Operation | Algorithm | Key Sizes |
|---|---|---|
| digital signature verification | ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 as defined in [FIPS_186_3] | 192 to 512 |
| digital signature verification | RSA PKCS#1 v1.5 with SHA-1, SHA-256 and SHA-512 | 1024, 1536, 2048, 3072 and 4096 |
| digital signature verification | RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512 | 1024, 1536, 2048, 3072 and 4096 |

**FCS_RND.1 Quality metric for random numbers**

**FCS_RND.1.1** The TSF shall provide a mechanism to generate random numbers that meet **the average Shannon entropy per internal random bit exceeds 0.994**.

### *9.1.3 Additional FCS SFR's Identified*

**FCS_CKM.1/CA_DATA_GEN Cryptographic key generation**

**FCS_CKM.1.1/CA_DATA_GEN** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below**

| Algorithm | Key Size | Standard |
|---|---|---|
| Chip Authentication Data Generation using DH keys compliant to PKCS#3 | 1024 to 2048 bits in steps of 512 bits | PKCS#3 |
| Chip authentication data generation using ECDH keys compliant to [ISO_15946] | 192 to 512 bits | [TR_03111] |

**FCS_CKM.1/GP Cryptographic key generation**

**FCS_CKM.1.1/GP** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **see table below** and specified cryptographic key sizes **see table below** that meet the following: **see table below:**

| Key Generation Algorithm | Key Sizes | Standard |
|---|---|---|
| Triple-DES in CBC mode | 112 bit | [GPC_SPE_034] |
| AES in CBC mode | 128, 192 and 256 | [GPC_SPE_014] |

**FCS_COP.1/GP_ENC Cryptographic operation**

**FCS_COP.1.1/GP_ENC** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

| Cryptographic Operation | Algorithm | Key Sizes | Standard |
|---|---|---|---|
| secure messaging (GP) – encryption and decryption | Triple-DES in CBC mode | 112 bit | [FIPS_46_3] |
| secure messaging (GP) – | AES in CBC | 128, 192 | [NIST_800_38A] |

| | | | |
|---|---|---|---|
| **encryption and decryption** | **mode** | **and 256 bits** | |

## FCS_COP.1/GP_AUTH Cryptographic operation

**FCS_COP.1.1/GP_AUTH** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

| Cryptographic Operation | Algorithm | Key Sizes | Standard |
|---|---|---|---|
| **symmetric authentication – message authentication code** | **Full 3DES MAC** | **112 bit** | **[ISO_9797_1]** |
| **symmetric authentication – message authentication code** | **AES CMAC** | **128, 192 and 256 bits** | **[NIST_800_38B]** |

## FCS_COP.1/GP_MAC Cryptographic operation

**FCS_COP.1.1/GP_MAC** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below**

| Cryptographic Operation | Algorithm | Key Size(s) | Standard |
|---|---|---|---|
| **secure messaging - message authentication code** | **Retail MAC** | **112 bit** | **[ISO_9797_1]** |
| **secure messaging (GP) - encryption and decryption** | **AES CMAC** | **128, 192 and 256 bits** | **[NIST_800_38B]** |

## FCS_COP.1/GP_KEY_DEC Cryptographic operation

**FCS_COP.1.1/GP_KEY_DEC** The TSF shall perform **see table below** in accordance with a specified cryptographic algorithm **see table below** and cryptographic key sizes **see table below** that meet the following: **see table below:**

| Cryptographic Operation | Algorithm | Key Sizes | Standard |
|---|---|---|---|
| **key decryption** | **Triple-DES in ECB mode** | **112 bit** | **[FIPS_46_3]** |
| **key decryption** | **AES in CBC mode** | **128, 192 and 256 bits** | **[FIPS_197]** |

**FCS_COP.1/AA Cryptographic operation**

**FCS_COP.1.1/AA** The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standard]**

| Cryptographic Operation | Cryptographic Algorithm | Cryptographic Key Sizes(bits) | Standard |
|---|---|---|---|
| Digital Signature Creation | ECDSA with SHA1, 256, 384, 512 | 192 to 521 over prime field curves | [ISO_9796-2], [PKCS#3], [FIPS_180_4] and [X.92] |
| Digital Signature Creation | RSA signature (CRT) with SHA1, 256, 384, 512 | 1024, 1536, 2048, 3072 and 4096 | [ISO_9796-2] |

### *9.1.4 Class FIA Identification and Authentication*

**FIA_UID.1 Timing of identification**

**FIA_UID.1.1** The TSF shall allow

- **to establish the communication channel,**
- **to read the Initialization Data if it is not disable by TSF according to FMT_MTD.1/INI_DIS**
- **to carry out the Chip Authentication Protocol**

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

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

**FIA_UAU.1 Timing of authentication**

**FIA_UAU.1.1** The TSF shall allow

- **to establish the communication channel,**
- **to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,**
- **to identify themselves by selection of the authentication key**
- **to carry out the Chip Authentication Protocol**

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

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

### FIA_UAU.4 Single-use authentication mechanisms

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

- **Terminal Authentication Protocol,**
- **Authentication Mechanism based on Triple-DES and AES**.

*Application Note:*

The authentication mechanisms based on Triple-DES and AES is the authentication process performed in phases 5 and 6

### FIA_UAU.5/EAC Multiple authentication mechanisms

**FIA_UAU.5.1/EAC** The TSF shall provide

- **Terminal Authentication Protocol,**
- **Secure messaging in MAC-ENC mode,**
- **Symmetric Authentication Mechanism based on Triple-DES and AES**

to support user authentication.

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

- **The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with Personalization Agent Key.**
- **After run of the Chip Authentication Protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.**
- **The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses the public key presented during the Chip Authentication Protocol and the secure messaging established by the Chip Authentication Mechanism**.

### FIA_UAU.6/EAC Re-authenticating

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

**FIA_API.1 Authentication Proof of Identity**

**FIA_API.1.1** The TSF shall provide a **Chip Authentication Protocol according to [TR_03110-3]** to prove the identity of the **TOE**.

### *9.1.5 Additional FIA SFR's Identified*

**FIA_UID.1/MP Timing of identification**

**FIA_UID.1.1/MP** The TSF shall allow

- **to carry out the authentication of the Manufacturer and Personalization Agent**

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

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

**FIA_UAU.1/MP Timing of authentication**

**FIA_UAU.1.1/MP** The TSF shall allow

- **to carry out the authentication of the Manufacturer and Personalization Agent**

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

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

**FIA_UAU.6/MP Re-authenticating**

**FIA_UAU.6.1/MP** The TSF shall re-authenticate the user under the conditions **each command sent to the TOE after successful authentication of the terminal with the Symmetric Authentication Mechanism shall be verified as being sent by the authenticated terminal**.

**FIA_AFL.1/MP Authentication failure handling**

**FIA_AFL.1.1/MP** The TSF shall detect when **1** unsuccessful authentication attempts occur related to **authentication of the Manufacturer and the Personalization Agent**.

**FIA_AFL.1.2/MP** When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **slow down exponentially the next authentication**.

### *9.1.6 Class FDP User Data Protection*

**FDP_ACC.1 Subset access control**

**FDP_ACC.1.1** The TSF shall enforce the **Access Control SFP** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD**.

**FDP_ACF.1 Security attribute based access control**

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

- **Subjects:**
  - **Personalization Agent,**
  - **Extended Inspection System**
  - **Terminal,**
- **Objects:**
  - **data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,**
  - **data EF.DG3 and EF.DG4 of the logical MRTD**
  - **data in EF.COM,**
  - **data in EF.SOD,**
- **Security attributes:**
  - **authentication status of terminals,**
  - **Terminal Authorization**.

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

- **the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,**
- **the successfully authenticated Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.**

- **the successfully authenticated Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG4 of the logical MRTD**.

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

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

- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,**
- **A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG3,**
- **A terminal authenticated as DV is not allowed to read data in the EF.DG4,**
- **Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,**
- **Any terminal not being successfully authenticated as Extended Inspection System is not allowed to read any of the EF.DG3 to EF.DG4 of the logical MRTD**.

**FDP_UCT.1/EAC Basic data exchange confidentiality**

**FDP_UCT.1.1/EAC [Editorially Refined]** The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure **after Chip Authentication**.

**FDP_UIT.1/EAC Data exchange integrity**

**FDP_UIT.1.1/EAC [Editorially Refined]** The TSF shall enforce the **Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors **after Chip Authentication**.

**FDP_UIT.1.2/EAC [Editorially Refined]** The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred **after Chip Authentication**.

### *9.1.7 Additional FDP SFR's Identified*

## FDP_ACC.1/UPD_FILE Subset access control

**FDP_ACC.1.1/UPD_FILE** The TSF shall enforce the **UPD_FILE Access Control SFP** on **terminals gaining write, read and modification access to data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

## FDP_ACF.1/UPD_FILE Security attribute based access control

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

- **Subjects:**
  - **Personalization Agent,**
  - **Extended Inspection System,**
  - **Terminal,**
- **Objects:**
  - **data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**
- **Security attributes**
  - **authentication status of terminals,**.

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

- **the Personalization Agent is allowed to write, read and modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD,**
- **the successfully authenticated Extended Inspection System with the name corresponding to the one (or beginning of the one) set following FMT_MTD.1.1/UPD_FILE is allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

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

**FDP_ACF.1.4/UPD_FILE** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any Terminal is not allowed to modify the data in the file(s) other than EF.COM, EF.SOD, and EF.DG1 to EF.DG16 of the logical MRTD**.

**FDP_DAU.1/AA Basic Data Authentication**

**FDP_DAU.1.1/AA** The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the TOE itself**.

**FDP_DAU.1.2/AA** The TSF shall provide **any users** with the ability to verify evidence of the validity of the indicated information.

**FDP_ITC.1/AA Import of user data without security attributes**

**FDP_ITC.1.1/AA** The TSF shall enforce the **Active Authentication Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP_ITC.1.2/AA** The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

**FDP_ITC.1.3/AA** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

### *9.1.8 Class FMT Security Management*

**FMT_SMF.1 Specification of Management Functions**

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

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

**FMT_SMR.1 Security roles**

**FMT_SMR.1.1** The TSF shall maintain the roles

- **Manufacturer,**
- **Personalization Agent,**
- **Country Verifying Certification Authority,**
- **Document Verifier,**
- **Domestic Extended Inspection System,**
- **Foreign Extended Inspection System,**
- **Administrator**.

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

### FMT_LIM.1 Limited capabilities

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

- **User Data to be manipulated or disclosed,**
- **TSF data to be manipulated or disclosed**
- **Software to be reconstructed,**
- **Substantial information about construction of TSF to be gathered which may enable other attacks,**
- **Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**

### FMT_LIM.2 Limited capabilities

**FMT_LIM.2.1** The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow,**

- **User Data to be manipulated or disclosed,**
- **TSF data to be manipulated or disclosed,**
- **Software to be reconstructed,**
- **Substantial information about construction of TSF to be gathered which may enable other attacks,**
- **Sensitive User Data (EF.DG3 and EF.DG4) to be disclosed**

### FMT_MTD.1/INI_ENA Management of TSF data

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

*Application Note:*

Please refer to F.ACW for details of the data written by the manufacturer.

### FMT_MTD.1/INI_DIS Management of TSF data

**FMT_MTD.1.1/INI_DIS** The TSF shall restrict the ability to **read out** the **Initialisation Data and the Pre-personalisation Data** to **the Personalization Agent**.

**FMT_MTD.1/CVCA_INI Management of TSF data**

**FMT_MTD.1.1/CVCA_INI** The TSF shall restrict the ability to **write** the
- **initial Country Verifying Certification Authority Public Key,**
- **initial Country Verifying Certification Authority Certificate,**
- **initial Current Date**

to **the Personalization Agent**.

**FMT_MTD.1/CVCA_UPD Management of TSF data**

**FMT_MTD.1.1/CVCA_UPD** The TSF shall restrict the ability to **update** the
- **Country Verifying Certification Authority Public Key,**
- **Country Verifying Certification Authority Certificate**

to **Country Verifying Certification Authority**.

**FMT_MTD.1/DATE Management of TSF data**

**FMT_MTD.1.1/DATE** The TSF shall restrict the ability to **modify** the **current date** to
- **Country Verifying Certification Authority,**
- **Document Verifier,**
- **Domestic Extended Inspection System**.

**FMT_MTD.1/KEY_WRITE Management of TSF data**

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

**FMT_MTD.1/CAPK Management of TSF data**

**FMT_MTD.1.1/CAPK** The TSF shall restrict the ability to **load** the **Chip Authentication Private Key** to **the Personalization agent**.

**FMT_MTD.1/KEY_READ Management of TSF data**

**FMT_MTD.1.1/KEY_READ** The TSF shall restrict the ability to **read** the
- **Document Basic Access Keys,**
- **Chip Authentication Private Key,**

- **Personalization Agent Keys,**
- **Manufacturer Keys**
- **Administrator Keys**

to **none**.

| **FMT_MTD.3 Secure TSF data** |
|---|

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

*Refinement:*

The certificate chain is valid if and only if

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

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

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

### *9.1.9 Additional FMT SFR's Identified*

| **FMT_MOF.1/AA Management of security functions behaviour** |
|---|

**FMT_MOF.1.1/AA** The TSF shall restrict the ability to **enable and disable** the functions **TSF Active Authentication** to **Personalization Agent**.

**FMT_MOF.1/GP Management of security functions behaviour**

**FMT_MOF.1.1/GP** The TSF shall restrict the ability to **enable** the functions

- **transmission of user data in a manner protected from unauthorised disclosure,**
- **reception of user data in a manner protected from unauthorised disclosure,**
- **transmission of user data in a manner protected from modification, deletion, insertion and replay errors,**
- **reception of user data in a manner protected from modification, deletion, insertion and replay errors,** to **the Manufacturer, Administrator and the Personalization Agent**.

**FMT_MTD.1/LCS_PERS Management of TSF data**

**FMT_MTD.1.1/LCS_PERS** The TSF shall restrict the ability to **switch** the **LCS from phase 6 to phase 7** to **the Personalization Agent**.

**FMT_MTD.1/UPD_FILE Management of TSF data**

**FMT_MTD.1.1/UPD_FILE** The TSF shall restrict the ability to **set** the **identifiers of files that can be modified in phase 7(different from EF.COM, EF.SOD, EF.DG1 to EF.DG16)** to **the Personalization Agent**.

**FMT_MTD.1/SM_LVL_DG3_DG4 Management of TSF data**

**FMT_MTD.1.1/SM_LVL_DG3_DG4** The TSF shall restrict the ability to **set** the **minimum Secure Messaging level required to access DG3 and DG4** to **the Personalization Agent**.

**FMT_MTD.1/SM_LVL Management of TSF data**

**FMT_MTD.1.1/SM_LVL** The TSF shall restrict the ability to **set** the **allowed Secure Messaging level when performing Chip Authentication** to **the Personalization Agent**.

*Application Note:*

Possible secure messaging levels are: 3DES, AES 128, AES 192 or AES 256

**FMT_MTD.1/AA_KEY_READ Management of TSF data**

**FMT_MTD.1.1/AA_KEY_READ** The TSF shall restrict the ability to **read** the **AAK** to **none**.

**FMT_MTD.1/AA_KEY_WRITE Management of TSF data**

**FMT_MTD.1.1/AA_KEY_WRITE** The TSF shall restrict the ability to **write** the **AAK** to **Personalization Agent**.

**FMT_MTD.1/ADMIN Management of TSF data**

**FMT_MTD.1.1/ADMIN** The TSF shall restrict the ability to **see table below** the **see table below** to **Admin**

| Operation | TSF Data |
|---|---|
| **Modify** | **The Chip Authentication key parameters to be used during key generation in USE phase** |
| **Invalidate** | **Invalidate one of the Chip Authentication key in USE phase or set the secondary key as being the primary key** |

**FMT_MTD.1/Key_Usage_Counter Management of TSF data**

**FMT_MTD.1.1/Key_Usage_Counter** The TSF shall restrict the ability to **configure** the **Key Usage Counter** to **Personalization Agent**.

### *9.1.10 Class FPT Protection of the Security Functions*

**FPT_EMS.1 TOE Emanation**

**FPT_EMS.1.1** The TOE shall not emit **power variations, timing variations during command execution** in excess of **non useful information** enabling access to **Personalization Agent Key(s) and Chip Authentication Private Key** and

- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys,**
- **Active Authentication: Private Key (AAK),**
- **Administrator Authentication Key(s)**.

**FPT_EMS.1.2** The TSF shall ensure **users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Key(s) and Chip Authentication Private Key** and

- **Pre-personalization Agent Keys,**
- **Secure Messaging Session Keys**
- **Active Authentication: Private Key (AAK),**
- **Administrator Authentication Key(s)**.

**FPT_FLS.1 Failure with preservation of secure state**

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

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

**FPT_TST.1 TSF testing**

**FPT_TST.1.1** The TSF shall run a suite of self tests **at the conditions**

- **At reset,** to demonstrate the correct operation of **the TSF**.

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

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

**FPT_PHP.3 Resistance to physical attack**

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

### *9.1.11 Class FTP Trusted path/channels*

## FTP_ITC.1/MP Inter-TSF trusted channel

**FTP_ITC.1.1/MP** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2/MP** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP_ITC.1.3/MP** The TSF shall initiate communication via the trusted channel for **loading sensitive data (Pre-Perso_K, Perso_K and CA_SK) shall be encrypted**.

## 9.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5.

### *9.2.1 ADV Development*

#### 9.2.1.1 ADV_ARC Security Architecture

**ADV_ARC.1 Security architecture description**

**ADV_ARC.1.1D** The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

**ADV_ARC.1.2D** The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

**ADV_ARC.1.3D** The developer shall provide a security architecture description of the TSF.

**ADV_ARC.1.1C** The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

**ADV_ARC.1.2C** The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

**ADV_ARC.1.3C** The security architecture description shall describe how the TSF initialisation process is secure.

**ADV_ARC.1.4C** The security architecture description shall demonstrate that the TSF protects itself from tampering.

**ADV_ARC.1.5C** The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

**ADV_ARC.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.1.2 ADV_FSP Functional specification

**ADV_FSP.5 Complete semi-formal functional specification with additional error information**

**ADV_FSP.5.1D** The developer shall provide a functional specification.

**ADV_FSP.5.2D** The developer shall provide a tracing from the functional specification to the SFRs.

**ADV_FSP.5.1C** The functional specification shall completely represent the TSF.

**ADV_FSP.5.2C** The functional specification shall describe the TSFI using a semi-formal style.

**ADV_FSP.5.3C** The functional specification shall describe the purpose and method of use for all TSFI.

**ADV_FSP.5.4C** The functional specification shall identify and describe all parameters associated with each TSFI.

**ADV_FSP.5.5C** The functional specification shall describe all actions associated with each TSFI.

**ADV_FSP.5.6C** The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

**ADV_FSP.5.7C** The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

**ADV_FSP.5.8C** The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

**ADV_FSP.5.9C** The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

**ADV_FSP.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV_FSP.5.2E** The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

#### 9.2.1.3 ADV_IMP Implementation representation

**ADV_IMP.1 Implementation representation of the TSF**

**ADV_IMP.1.1D** The developer shall make available the implementation representation for the entire TSF.

**ADV_IMP.1.2D** The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

**ADV_IMP.1.1C** The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

**ADV_IMP.1.2C** The implementation representation shall be in the form used by the development personnel.

**ADV_IMP.1.3C** The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

**ADV_IMP.1.1E** The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

#### 9.2.1.4 ADV_INT TSF internals

| **ADV_INT.2 Well-structured internals** |
|---|

**ADV_INT.2.1D** The developer shall design and implement the entire TSF such that it has well-structured internals.

**ADV_INT.2.2D** The developer shall provide an internals description and justification.

**ADV_INT.2.1C** The justification shall describe the characteristics used to judge the meaning of ``well-structured".

**ADV_INT.2.2C** The TSF internals description shall demonstrate that the entire TSF is well-structured.

**ADV_INT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV_INT.2.2E** The evaluator shall perform an internals analysis on the TSF.

#### 9.2.1.5 ADV_TDS TOE design

**ADV_TDS.4 Semiformal modular design**

**ADV_TDS.4.1D** The developer shall provide the design of the TOE.

**ADV_TDS.4.2D** The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

**ADV_TDS.4.1C** The design shall describe the structure of the TOE in terms of subsystems.

**ADV_TDS.4.2C** The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

**ADV_TDS.4.3C** The design shall identify all subsystems of the TSF.

**ADV_TDS.4.4C** The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

**ADV_TDS.4.5C** The design shall provide a description of the interactions among all subsystems of the TSF.

**ADV_TDS.4.6C** The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

**ADV_TDS.4.7C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

**ADV_TDS.4.8C** The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

**ADV_TDS.4.9C** The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

**ADV_TDS.4.10C** The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

**ADV_TDS.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ADV_TDS.4.2E** The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

### *9.2.2 AGD Guidance documents*

#### 9.2.2.1 AGD_OPE Operational user guidance

| **AGD_OPE.1 Operational user guidance** |
|---|

**AGD_OPE.1.1D** The developer shall provide operational user guidance.

**AGD_OPE.1.1C** The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

**AGD_OPE.1.2C** The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

**AGD_OPE.1.3C** The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

**AGD_OPE.1.4C** The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

**AGD_OPE.1.5C** The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

**AGD_OPE.1.6C** The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

**AGD_OPE.1.7C** The operational user guidance shall be clear and reasonable.

**AGD_OPE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.2.2 AGD_PRE Preparative procedures

| **AGD_PRE.1 Preparative procedures** |
|---|

**AGD_PRE.1.1D** The developer shall provide the TOE including its preparative procedures.

**AGD_PRE.1.1C** The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

**AGD_PRE.1.2C** The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

**AGD_PRE.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AGD_PRE.1.2E** The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

### *9.2.3 ALC Life-cycle support*

#### 9.2.3.1 ALC_CMC CM capabilities

**ALC_CMC.4 Production support, acceptance procedures and automation**

**ALC_CMC.4.1D** The developer shall provide the TOE and a reference for the TOE.

**ALC_CMC.4.2D** The developer shall provide the CM documentation.

**ALC_CMC.4.3D** The developer shall use a CM system.

**ALC_CMC.4.1C** The TOE shall be labelled with its unique reference.

**ALC_CMC.4.2C** The CM documentation shall describe the method used to uniquely identify the configuration items.

**ALC_CMC.4.3C** The CM system shall uniquely identify all configuration items.

**ALC_CMC.4.4C** The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

**ALC_CMC.4.5C** The CM system shall support the production of the TOE by automated means.

**ALC_CMC.4.6C** The CM documentation shall include a CM plan.

**ALC_CMC.4.7C** The CM plan shall describe how the CM system is used for the development of the TOE.

**ALC_CMC.4.8C** The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

**ALC_CMC.4.9C** The evidence shall demonstrate that all configuration items are being maintained under the CM system.

**ALC_CMC.4.10C** The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

**ALC_CMC.4.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.3.2 ALC_CMS CM scope

**ALC_CMS.5 Development tools CM coverage**

**ALC_CMS.5.1D** The developer shall provide a configuration list for the TOE.

**ALC_CMS.5.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

**ALC_CMS.5.2C** The configuration list shall uniquely identify the configuration items.

**ALC_CMS.5.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

**ALC_CMS.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.3.3 ALC_DEL Delivery

**ALC_DEL.1 Delivery procedures**

**ALC_DEL.1.1D** The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

**ALC_DEL.1.2D** The developer shall use the delivery procedures.

**ALC_DEL.1.1C** The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

**ALC_DEL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.3.4 ALC_DVS Development security

**ALC_DVS.2 Sufficiency of security measures**

**ALC_DVS.2.1D** The developer shall produce and provide development security documentation.

**ALC_DVS.2.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

**ALC_DVS.2.2C** The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

**ALC_DVS.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC_DVS.2.2E** The evaluator shall confirm that the security measures are being applied.

#### 9.2.3.5 ALC_FLR Flaw remediation

**ALC_FLR.1 Basic flaw remediation**

**ALC_FLR.1.1D** The developer shall document and provide flaw remediation procedures addressed to TOE developers.

**ALC_FLR.1.1C** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

**ALC_FLR.1.2C** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

**ALC_FLR.1.3C** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

**ALC_FLR.1.4C** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective action to TOE users.

**ALC_FLR.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.3.6 ALC_LCD Life-cycle definition

**ALC_LCD.1 Developer defined life-cycle model**

**ALC_LCD.1.1D** The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

**ALC_LCD.1.2D** The developer shall provide life-cycle definition documentation.

**ALC_LCD.1.1C** The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

**ALC_LCD.1.2C** The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

**ALC_LCD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 9.2.3.7 ALC_TAT Tools and techniques

**ALC_TAT.2 Compliance with implementation standards**

**ALC_TAT.2.1D** The developer shall provide the documentation identifying each development tool being used for the TOE.

**ALC_TAT.2.2D** The developer shall document and provide the selected implementation-dependent options of each development tool.

**ALC_TAT.2.3D** The developer shall describe and provide the implementation standards that are being applied by the developer.

**ALC_TAT.2.1C** Each development tool used for implementation shall be well-defined.

**ALC_TAT.2.2C** The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

**ALC_TAT.2.3C** The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

**ALC_TAT.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ALC_TAT.2.2E** The evaluator shall confirm that the implementation standards have been applied.

### *9.2.4 ASE Security Target evaluation*

#### 9.2.4.1 ASE_CCL Conformance claims

**ASE_CCL.1 Conformance claims**

**ASE_CCL.1.1D** The developer shall provide a conformance claim.

**ASE_CCL.1.2D** The developer shall provide a conformance claim rationale.

**ASE_CCL.1.1C** The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

**ASE_CCL.1.2C** The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

**ASE_CCL.1.3C** The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

**ASE_CCL.1.4C** The CC conformance claim shall be consistent with the extended components definition.

**ASE_CCL.1.5C** The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

**ASE_CCL.1.6C** The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

**ASE_CCL.1.7C** The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

**ASE_CCL.1.8C** The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

**ASE_CCL.1.9C** The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

**ASE_CCL.1.10C** The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

**ASE_CCL.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.4.2 ASE_ECD Extended components definition

**ASE_ECD.1 Extended components definition**

**ASE_ECD.1.1D** The developer shall provide a statement of security requirements.

**ASE_ECD.1.2D** The developer shall provide an extended components definition.

**ASE_ECD.1.1C** The statement of security requirements shall identify all extended security requirements.

**ASE_ECD.1.2C** The extended components definition shall define an extended component for each extended security requirement.

**ASE_ECD.1.3C** The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

**ASE_ECD.1.4C** The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

**ASE_ECD.1.5C** The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

**ASE_ECD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE_ECD.1.2E** The evaluator shall confirm that no extended component can be clearly expressed using existing components.

#### 9.2.4.3 ASE_INT ST introduction

| **ASE_INT.1 ST introduction** |
|---|

**ASE_INT.1.1D** The developer shall provide an ST introduction.

**ASE_INT.1.1C** The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

**ASE_INT.1.2C** The ST reference shall uniquely identify the ST.

**ASE_INT.1.3C** The TOE reference shall identify the TOE.

**ASE_INT.1.4C** The TOE overview shall summarise the usage and major security features of the TOE.

**ASE_INT.1.5C** The TOE overview shall identify the TOE type.

**ASE_INT.1.6C** The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

**ASE_INT.1.7C** The TOE description shall describe the physical scope of the TOE.

**ASE_INT.1.8C** The TOE description shall describe the logical scope of the TOE.

**ASE_INT.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE_INT.1.2E** The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

#### 9.2.4.4 ASE_OBJ Security objectives

**ASE_OBJ.2 Security objectives**

**ASE_OBJ.2.1D** The developer shall provide a statement of security objectives.

**ASE_OBJ.2.2D** The developer shall provide a security objectives rationale.

**ASE_OBJ.2.1C** The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

**ASE_OBJ.2.2C** The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

**ASE_OBJ.2.3C** The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

**ASE_OBJ.2.4C** The security objectives rationale shall demonstrate that the security objectives counter all threats.

**ASE_OBJ.2.5C** The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

**ASE_OBJ.2.6C** The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

**ASE_OBJ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.4.5 ASE_REQ Security requirements

| **ASE_REQ.2 Derived security requirements** |
|---|

**ASE_REQ.2.1D** The developer shall provide a statement of security requirements.

**ASE_REQ.2.2D** The developer shall provide a security requirements rationale.

**ASE_REQ.2.1C** The statement of security requirements shall describe the SFRs and the SARs.

**ASE_REQ.2.2C** All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

**ASE_REQ.2.3C** The statement of security requirements shall identify all operations on the security requirements.

**ASE_REQ.2.4C** All operations shall be performed correctly.

**ASE_REQ.2.5C** Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

**ASE_REQ.2.6C** The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

**ASE_REQ.2.7C** The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

**ASE_REQ.2.8C** The security requirements rationale shall explain why the SARs were chosen.

**ASE_REQ.2.9C** The statement of security requirements shall be internally consistent.

**ASE_REQ.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.4.6 ASE_SPD Security problem definition

**ASE_SPD.1 Security problem definition**

**ASE_APD.1.1D** The developer shall provide a security problem definition.

**ASE_SPD.1.1C** The security problem definition shall describe the threats.

**ASE_SPD.1.2C** All threats shall be described in terms of a threat agent, an asset, and an adverse action.

**ASE_SPD.1.3C** The security problem definition shall describe the OSPs.

**ASE_SPD.1.4C** The security problem definition shall describe the assumptions about the operational environment of the TOE.

**ASE_SPD.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.4.7 ASE_TSS TOE summary specification

**ASE_TSS.1 TOE summary specification**

**ASE_TSS.1.1D** The developer shall provide a TOE summary specification.

**ASE_TSS.1.1C** The TOE summary specification shall describe how the TOE meets each SFR.

**ASE_TSS.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ASE_TSS.1.2E** The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

### *9.2.5 ATE Tests*

#### 9.2.5.1 ATE_COV Coverage

| **ATE_COV.2 Analysis of coverage** |
|---|

**ATE_COV.2.1D** The developer shall provide an analysis of the test coverage.

**ATE_COV.2.1C** The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

**ATE_COV.2.2C** The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

**ATE_COV.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.5.2 ATE_DPT Depth

| **ATE_DPT.3 Testing: modular design** |
|---|

**ATE_DPT.3.1D** The developer shall provide the analysis of the depth of testing.

**ATE_DPT.3.1C** The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

**ATE_DPT.3.2C** The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

**ATE_DPT.3.3C** The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

**ATE_DPT.3.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.5.3 ATE_FUN Functional tests

**ATE_FUN.1 Functional testing**

**ATE_FUN.1.1D** The developer shall test the TSF and document the results.

**ATE_FUN.1.2D** The developer shall provide test documentation.

**ATE_FUN.1.1C** The test documentation shall consist of test plans, expected test results and actual test results.

**ATE_FUN.1.2C** The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

**ATE_FUN.1.3C** The expected test results shall show the anticipated outputs from a successful execution of the tests.

**ATE_FUN.1.4C** The actual test results shall be consistent with the expected test results.

**ATE_FUN.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### 9.2.5.4 ATE_IND Independent testing

| **ATE_IND.2 Independent testing - sample** |
|---|

**ATE_IND.2.1D** The developer shall provide the TOE for testing.

**ATE_IND.2.1C** The TOE shall be suitable for testing.

**ATE_IND.2.2C** The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

**ATE_IND.2.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**ATE_IND.2.2E** The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

**ATE_IND.2.3E** The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

### *9.2.6 AVA Vulnerability assessment*

#### 9.2.6.1 AVA_VAN Vulnerability analysis

**AVA_VAN.5 Advanced methodical vulnerability analysis**

**AVA_VAN.5.1D** The developer shall provide the TOE for testing.

**AVA_VAN.5.1C** The TOE shall be suitable for testing.

**AVA_VAN.5.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

**AVA_VAN.5.2E** The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

**AVA_VAN.5.3E** The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

**AVA_VAN.5.4E** The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

## 9.3 Security Requirements Rationale

### *9.3.1 Objectives*

#### 9.3.1.1 Security Objectives for the TOE

**Security Objectives from Protection Profile**

**OT.AC_Pers** The security objective OT.AC_Pers "Access Control for Personalization of logical MRTD" addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FIA_UID.1, FIA_UID.1/MP, FIA_UAU.1, FIA_UAU.1/MP FDP_ACC.1 and FDP_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT_MTD.1/KEY_WRITE as authentication reference data for Basic Access Control.

The following paragraph is extracted from [PP_EAC] and has been refined according to the technical characteristics of this TOE. The refinement is right after.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/EAC. If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA, FCS_CKM.1/CA_DATA_GEN for generation of CA Data in phase 6, FCS_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol) and FIA_UAU.6/EAC (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/GP_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

Note: As TA mechanism is not supported for the authentication of the terminal as Personalization Agent, the following two paragraphs have been added to demonstrate that symmetric authentication used in Personalization phase fulfills the OT.AC_Pers. The authentication of the terminal as Personalization Agent is performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/EAC. The Personalization Agent can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the personalization key. FIA_UAU.6/MP describes the re-authentication. In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack.

As the symmetric authentication is used in Personalization phase, the SFR FIA_UAU.6/MP describes the re-authentication. Secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC as well as FCS_COP.1/GP_MAC for the ENC_MAC_Mode. The SFR FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

The SFR FMT_MTD.1/KEY_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT_EMS.1 the confidentially of these keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1 and FDP_ACF.1. The Personalization Agent is the only subject allowed to ends Personalization of logical MRTD, setting the TOE Life Cycle State in Operational Use state according to FMT_MTD.1/LCS_PERS. Since then it is no more possible to return in Personalization state.

**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 and FDP_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA_UID.1, FIA_UID.1/MP, FIA_UAU.1 and FIA_UAU.1/MP before accessing these data. The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA_UAU.4, FIA_UAU.5/EAC and FIA_UAU.6/EAC. The SFR FIA_UAU.6/EAC and FDP_UIT.1/EACA requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret), FCS_COP.1/SHA (for the derivation of the new session keys), and FCS_COP.1/SYM and FCS_COP.1/MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Data_Int.

Manufacturer and Personalization Agent are also able to detect any modification of the transmitted logical MRTD data by means of the Symmetric Authentication mechanism. The SFR FIA_UAU.6/MP and FMT_MOF.1/GP requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC for the ENC_MAC_Mode. FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1 and FDP_ACF.1.

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

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

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

The following part is added to integrate the Manufacturing and Personalization phases in the OT_Sens_Data_Conf.

Manufacturer and Personalization Agent are also able to detect any modification of the transmitted logical MRTD data by means of the Symmetric Authentication mechanism. The SFR FIA_UAU.6/MP, and FMT_MOF.1/GP requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC for the ENC_MAC_Mode. FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

SFR FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE define rules to manage files different from the ones managed by FDP_ACC.1 and FDP_ACF.1.

**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 (including the Personalization Agent key). The SFR FMT_MTD.1/INI_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 "Operational Use" violates the security objective OT.Identification "Identification and Authentication of the TOE".

**OT.Chip_Auth_Proof** The security objective OT.Chip_Auth_Proof "Proof of MRTD's chip authenticity" is ensured by the Chip Authentication Protocol provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Data

is generated by using FCS_CKM.1/CA_DATA_GEN. The Chip Authentication Protocol [TR_03110-3] requires additional TSF according to FCS_COP.1/SHA (for the derivation of the session keys), FCS_COP.1/SYM and FCS_COP.1/MAC (for the ENC_MAC_Mode secure messaging).

**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 features which may not be used after TOE Delivery.

**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/or processed in the MRTD's chip against disclosure

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

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

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

**Additional Security Objectives Identified**

**OT.Configuration** The security objective OT.Configuration "Protection of the TOE preparation" addresses management of the Data Configuration, Pre-personalization Agent keys, Personalization Agent keys and the Life Cycle State of the TOE.

The authentication of the terminal as Manufacturer is performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/EAC. The Manufacturer can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the Pre-personalization key. FIA_UAU.6/MP describes the re-authentication. In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack. The SFR FTP_ITC.1/MP allows the Manufacturer to communicate with the OS.

Once step 4 is done, the MRTD packaging responsible is allowed to set the Pre-personalization Agent keys according to the SFR FCS_COP.1/GP_KEY_DEC. The read access to the Pre-personalization keys is prevented by SFRs FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3 the confidentially of these keys.

In step 5, the authentication of the terminal as Manufacturer shall be performed by TSF according to SFR FIA_UAU.4 and FIA_UAU.5/EAC. The Manufacturer shall be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH).

In case of failed authentication attempts FIA_AFL.1/MP enforces additional waiting time prolonging the necessary amount of time for facilitating a brute force attack

The SFR FIA_UAU.6/MP describes the re-authentication and the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/GP, FCS_RND.1 (for key generation), and FCS_COP.1/GP_ENC as well as FCS_COP.1/GP_MAC for the ENC_MAC_Mode. The SFR FCS_CKM.4 enforces the destruction of Secure Messaging session keys.

The Personalization Agent can enable the modification of files in operational use phase according to FMT_MTD.1/UPD_FILE.

The SFR FMT_SMR.1 lists the roles and the SFR FMT_SMF.1 lists the TSF management functions setting the Pre-personalization Agent Keys. The read access to the secret key of the Personalization Agent Keys is prevented by the SFRs FCS_CKM.4, FPT_EMS.1, FPT_FLS.1 and FPT_PHP.3.

Since then it is no more possible to return in manufacturing state and the role Manufacturer is no longer available as FCS_CKM.4 destroys Manufacturer keys.

**OT.Update_File** The security objective OT.Update_File deals with the capability to update date in the operational phase after a succesful authentication. This objective is enforced by FMT_MTD.1/UPD_FILE thatensures only the terminal specified by the personalization agent can update the data in the operational phase.

FDP_ACC.1/UPD_FILE and FDP_ACF.1/UPD_FILE enforce the acccess conditions that are required to be fulfilled before data is updated.

**OT.AC_SM_Level** The security objective OT.AC_SM_Level "Access control to sensitive biometric reference data according to SM level" is covered by FMT_MTD.1/SM_LVL_DG3_DG4 and FMT_MTD.1/SM_LVL that allows the personalization agent to set the SM level required to access to the sensitive data.

**OT.AA_Proof** The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by FMT_MOF.1/AA and provided by FDP_DAU.1/AA, FDP_ITC.1/AA proving the identity and authenticity of the TOE. The Active Authentication relies on FCS_COP.1/AA and FCS_RND.1. It is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/AA_KEY_WRITE and FMT_MTD.1/AA_KEY_READ.

**OT.Data_Int_AA** The security objective OT.AA_Proof is ensured by the Active Authentication Protocol activated by FMT_MOF.1/AA and provided by FDP_DAU.1/AA and FDP_ITC.1/AA proving the identity and authenticity of the TOE.

**OT.ADMIN_Configuration** The security objective OT.ADMIN_Configuration "Protection of the TOE administration" addresses management of the Data Configuration with key size management for the Chip Authentication of the TOE. The Administrator can be authenticated by using the symmetric authentication mechanism (FCS_COP.1/GP_AUTH) with the Administartor key. ADMIN keys are created during pre-personalization. FMT_MTD.1/KEY_READ restricts the ability to read the Administrator Keys to none. The Administartor can select the protection mode of user data following FMT_MOF.1/GP. FPT_EMS.1 protects the confidentially of Administrator Agent keys. The SFRs FMT_SMF.1 and FMT_SMR.1 support the functions and roles related. The administration TSF data manipulation are supported by FMT_MTD.1/ADMIN. It is now allowed to modify the Chip

Authentication key parameters to be used during key generation in USE phase. The minimum key size that the user can generate in USE phase is controlled by the "ADMIN" role. It is also possible to change the key parameters during the key generation process. For example changing the domain parameters of an elliptic curve key. It is also possible to invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key. Note: after such process, the "freed" CA key set is available for a future CA key generation.

**OT.Key_Usage_Counter** The security objective OT.Key_Usage_Counter is covered by FMT_MTD.1/Key_Usage_Counter.

### *9.3.2 Rationale tables of Security Objectives and SFRs*

| Security Objectives | Security Functional Requirements | Rationale |
|---|---|---|
| OT.AC_Pers | FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FIA_AFL.1/MP, FDP_ACC.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1, FDP_ACF.1/UPD_FILE, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/KEY_READ, FMT_MTD.1/LCS_PERS, FPT_EMS.1, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_RND.1, FCS_CKM.1/CA_DATA_GEN, FIA_UID.1/MP, FIA_UAU.1/MP | Section 9.3.1 |
| OT.Data_Int | FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FDP_UIT.1/EAC, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1/GP, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_CKM.1/GP, FCS_RND.1, FIA_UID.1/MP, FIA_UAU.1/MP | Section 9.3.1 |
| OT.Sens_Data_Conf | FCS_CKM.1/CA, FCS_CKM.4, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UID.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FDP_UCT.1/EAC, FMT_MOF.1/GP, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FMT_MTD.3, | Section 9.3.1 |

| | | |
|---|---|---|
| | FCS_CKM.1/GP, FCS_RND.1, FCS_CKM.1/CA_DATA_GEN | |
| OT.Identification | FAU_SAS.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS | Section 9.3.1 |
| OT.Chip_Auth_Proof | FCS_CKM.1/CA, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FIA_API.1, FMT_MTD.1/CAPK, FMT_MTD.1/KEY_READ, FCS_CKM.1/CA_DATA_GEN | Section 9.3.1 |
| OT.Prot_Abuse-Func | FMT_LIM.1, FMT_LIM.2 | Section 9.3.1 |
| OT.Prot_Inf_Leak | FPT_EMS.1, FPT_FLS.1, FPT_TST.1, FPT_PHP.3 | Section 9.3.1 |
| OT.Prot_Phys-Tamper | FPT_PHP.3 | Section 9.3.1 |
| OT.Prot_Malfunction | FPT_TST.1, FPT_FLS.1 | Section 9.3.1 |
| OT.Configuration | FCS_CKM.1/GP, FCS_COP.1/GP_ENC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_MAC, FCS_COP.1/GP_KEY_DEC, FIA_UAU.6/MP, FIA_AFL.1/MP, FCS_CKM.4, FIA_UAU.4, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/UPD_FILE, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3, FCS_RND.1, FIA_UAU.5/EAC, FTP_ITC.1/MP | Section 9.3.1 |
| OT.Update_File | FMT_MTD.1/UPD_FILE, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE | Section 9.3.1 |
| OT.AC_SM_Level | FMT_MTD.1/SM_LVL_DG3_DG4, FMT_MTD.1/SM_LVL | Section 9.3.1 |
| OT.AA_Proof | FCS_COP.1/AA, FCS_RND.1, FDP_DAU.1/AA, FDP_ITC.1/AA, FMT_MOF.1/AA, FMT_MTD.1/AA_KEY_READ, FMT_MTD.1/AA_KEY_WRITE | Section 9.3.1 |
| OT.Data_Int_AA | FDP_DAU.1/AA, FDP_ITC.1/AA, FMT_MOF.1/AA | Section 9.3.1 |
| OT.ADMIN_Configuration | FCS_COP.1/GP_AUTH, FMT_MTD.1/KEY_READ, FMT_MOF.1/GP, FPT_EMS.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/ADMIN | Section 9.3.1 |
| OT.Key_Usage_Counter | FMT_MTD.1/Key_Usage_Counter | Section 9.3.1 |

**Table 20 Security Objectives and SFRs - Coverage**

| Security Functional Requirements | Security Objectives |
|---|---|
| FAU_SAS.1 | OT.Identification |
| FCS_CKM.1/CA | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FCS_CKM.4 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |

| | |
|---|---|
| FCS_COP.1/SHA | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FCS_COP.1/SYM | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FCS_COP.1/MAC | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FCS_COP.1/SIG_VER | OT.AC_Pers, OT.Sens_Data_Conf |
| FCS_RND.1 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration, OT.AA_Proof |
| FCS_CKM.1/CA_DATA_GEN | OT.AC_Pers, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FCS_CKM.1/GP | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FCS_COP.1/GP_ENC | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FCS_COP.1/GP_AUTH | OT.AC_Pers, OT.Configuration, OT.ADMIN_Configuration |
| FCS_COP.1/GP_MAC | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FCS_COP.1/GP_KEY_DEC | OT.Configuration |
| FCS_COP.1/AA | OT.AA_Proof |
| FIA_UID.1 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf |
| FIA_UAU.1 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf |
| FIA_UAU.4 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FIA_UAU.5/EAC | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FIA_UAU.6/EAC | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf |
| FIA_API.1 | OT.Chip_Auth_Proof |
| FIA_UID.1/MP | OT.AC_Pers, OT.Data_Int |
| FIA_UAU.1/MP | OT.AC_Pers, OT.Data_Int |
| FIA_UAU.6/MP | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Configuration |
| FIA_AFL.1/MP | OT.AC_Pers, OT.Configuration |
| FDP_ACC.1 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf |
| FDP_ACF.1 | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf |
| FDP_UCT.1/EAC | OT.Sens_Data_Conf |
| FDP_UIT.1/EAC | OT.Data_Int |

| | |
|---|---|
| FDP_ACC.1/UPD_FILE | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Update_File |
| FDP_ACF.1/UPD_FILE | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Update_File |
| FDP_DAU.1/AA | OT.AA_Proof, OT.Data_Int_AA |
| FDP_ITC.1/AA | OT.AA_Proof, OT.Data_Int_AA |
| FMT_SMF.1 | OT.AC_Pers, OT.Data_Int, OT.Configuration, OT.ADMIN_Configuration |
| FMT_SMR.1 | OT.AC_Pers, OT.Data_Int, OT.Configuration, OT.ADMIN_Configuration |
| FMT_LIM.1 | OT.Prot_Abuse-Func |
| FMT_LIM.2 | OT.Prot_Abuse-Func |
| FMT_MTD.1/INI_ENA | OT.Identification |
| FMT_MTD.1/INI_DIS | OT.Identification |
| FMT_MTD.1/CVCA_INI | OT.Sens_Data_Conf |
| FMT_MTD.1/CVCA_UPD | OT.Sens_Data_Conf |
| FMT_MTD.1/DATE | OT.Sens_Data_Conf |
| FMT_MTD.1/KEY_WRITE | OT.AC_Pers |
| FMT_MTD.1/CAPK | OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof |
| FMT_MTD.1/KEY_READ | OT.AC_Pers, OT.Data_Int, OT.Sens_Data_Conf, OT.Chip_Auth_Proof, OT.ADMIN_Configuration |
| FMT_MTD.3 | OT.Sens_Data_Conf |
| FMT_MOF.1/AA | OT.AA_Proof, OT.Data_Int_AA |
| FMT_MOF.1/GP | OT.Data_Int, OT.Sens_Data_Conf, OT.ADMIN_Configuration |
| FMT_MTD.1/LCS_PERS | OT.AC_Pers |
| FMT_MTD.1/UPD_FILE | OT.Configuration, OT.Update_File |
| FMT_MTD.1/SM_LVL_DG3_DG4 | OT.AC_SM_Level |
| FMT_MTD.1/SM_LVL | OT.AC_SM_Level |
| FMT_MTD.1/AA_KEY_READ | OT.AA_Proof |
| FMT_MTD.1/AA_KEY_WRITE | OT.AA_Proof |
| FMT_MTD.1/ADMIN | OT.ADMIN_Configuration |
| FMT_MTD.1/Key_Usage_Counter | OT.Key_Usage_Counter |
| FPT_EMS.1 | OT.AC_Pers, OT.Prot_Inf_Leak, OT.Configuration, OT.ADMIN_Configuration |
| FPT_FLS.1 | OT.Prot_Inf_Leak, OT.Prot_Malfunction, |

| | |
|---|---|
| | OT.Configuration |
| FPT_TST.1 | OT.Prot_Inf_Leak, OT.Prot_Malfunction |
| FPT_PHP.3 | OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper, OT.Configuration |
| FTP_ITC.1/MP | OT.Configuration |

**Table 21 SFRs and Security Objectives**

### *9.3.3 Dependencies*

#### 9.3.3.1 SFRs Dependencies

| Requirements | CC Dependencies | Satisfied Dependencies |
|---|---|---|
| FAU_SAS.1 | No Dependencies | |
| FCS_CKM.1/CA | (FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4) | FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC |
| FCS_CKM.4 | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) | FCS_CKM.1/CA, FCS_CKM.1/GP |
| FCS_COP.1/SHA | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.4 |
| FCS_COP.1/SYM | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.1/CA, FCS_CKM.4 |
| FCS_COP.1/MAC | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.1/CA, FCS_CKM.4 |
| FCS_COP.1/SIG_VER | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.1/CA, FCS_CKM.4 |
| FCS_RND.1 | No Dependencies | |
| FCS_CKM.1/CA_DATA_GEN | (FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4) | FCS_CKM.4, FCS_COP.1/SIG_VER |
| FCS_CKM.1/GP | (FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4) | FCS_CKM.4, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC |
| FCS_COP.1/GP_ENC | (FCS_CKM.1 or | FCS_CKM.4, FCS_CKM.1/GP |

| | | |
|---|---|---|
| | FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | |
| FCS_COP.1/GP_AUTH | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.4, FCS_CKM.1/GP |
| FCS_COP.1/GP_MAC | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.4, FCS_CKM.1/GP |
| FCS_COP.1/GP_KEY_DEC | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.4, FCS_CKM.1/GP |
| FCS_COP.1/AA | (FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4) | FCS_CKM.4, FDP_ITC.1/AA |
| FIA_UID.1 | No Dependencies | |
| FIA_UAU.1 | (FIA_UID.1) | FIA_UID.1 |
| FIA_UAU.4 | No Dependencies | |
| FIA_UAU.5/EAC | No Dependencies | |
| FIA_UAU.6/EAC | No Dependencies | |
| FIA_API.1 | No Dependencies | |
| FIA_UID.1/MP | No Dependencies | |
| FIA_UAU.1/MP | (FIA_UID.1) | FIA_UID.1/MP |
| FIA_UAU.6/MP | No Dependencies | |
| FIA_AFL.1/MP | (FIA_UAU.1) | FIA_UAU.1/MP |
| FDP_ACC.1 | (FDP_ACF.1) | FDP_ACF.1 |
| FDP_ACF.1 | (FDP_ACC.1) and (FMT_MSA.3) | FDP_ACC.1 |
| FDP_UCT.1/EAC | (FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1) | FDP_ACC.1 |
| FDP_UIT.1/EAC | (FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1) | FDP_ACC.1 |
| FDP_ACC.1/UPD_FILE | (FDP_ACF.1) | FDP_ACF.1/UPD_FILE |

| | | |
|---|---|---|
| FDP_ACF.1/UPD_FILE | (FDP_ACC.1) and (FMT_MSA.3) | FDP_ACC.1/UPD_FILE |
| FDP_DAU.1/AA | No Dependencies | |
| FDP_ITC.1/AA | (FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3) | FDP_ACC.1 |
| FMT_SMF.1 | No Dependencies | |
| FMT_SMR.1 | (FIA_UID.1) | FIA_UID.1 |
| FMT_LIM.1 | (FMT_LIM.2) | FMT_LIM.2 |
| FMT_LIM.2 | (FMT_LIM.1) | FMT_LIM.1 |
| FMT_MTD.1/INI_ENA | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/INI_DIS | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/CVCA_INI | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/CVCA_UPD | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/DATE | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/KEY_WRITE | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/CAPK | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/KEY_READ | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.3 | (FMT_MTD.1) | FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD |
| FMT_MOF.1/AA | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MOF.1/GP | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/LCS_PERS | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/UPD_FILE | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/SM_LVL_DG3_DG4 | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/SM_LVL | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |

| | | |
|---|---|---|
| FMT_MTD.1/AA_KEY_READ | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/AA_KEY_WRITE | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/ADMIN | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FMT_MTD.1/Key_Usage_Counter | (FMT_SMF.1) and (FMT_SMR.1) | FMT_SMF.1, FMT_SMR.1 |
| FPT_EMS.1 | No Dependencies | |
| FPT_FLS.1 | No Dependencies | |
| FPT_TST.1 | No Dependencies | |
| FPT_PHP.3 | No Dependencies | |
| FTP_ITC.1/MP | No Dependencies | |

**Table 22 SFRs Dependencies**

**Rationale for the exclusion of Dependencies**

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

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

**The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UCT.1/EAC is discarded.** The SFR FDP_UCT.1/EAC requires the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

**The dependency FTP_ITC.1 or FTP_TRP.1 of FDP_UIT.1/EAC is discarded.** The SFR FDP_UIT.1/EAC requires the use secure messaging between the MRTD and the GIS. There is no need for the SFR FTP_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP_TRP.1 is not applicable here.

**The dependency FMT_MSA.3 of FDP_ACF.1/UPD_FILE is discarded.** The access control TSF according to FDP_ACF.1/UPD_FILE uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No

management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

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

#### 9.3.3.2 SARs Dependencies

| Requirements | CC Dependencies | Satisfied Dependencies |
|---|---|---|
| ADV_ARC.1 | (ADV_FSP.1) and (ADV_TDS.1) | ADV_FSP.5, ADV_TDS.4 |
| ADV_FSP.5 | (ADV_IMP.1) and (ADV_TDS.1) | ADV_IMP.1, ADV_TDS.4 |
| ADV_IMP.1 | (ADV_TDS.3) and (ALC_TAT.1) | ADV_TDS.4, ALC_TAT.2 |
| ADV_INT.2 | (ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1) | ADV_IMP.1, ADV_TDS.4, ALC_TAT.2 |
| ADV_TDS.4 | (ADV_FSP.5) | ADV_FSP.5 |
| AGD_OPE.1 | (ADV_FSP.1) | ADV_FSP.5 |
| AGD_PRE.1 | No Dependencies | |
| ALC_CMC.4 | (ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1) | ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 |
| ALC_CMS.5 | No Dependencies | |
| ALC_DEL.1 | No Dependencies | |
| ALC_DVS.2 | No Dependencies | |
| ALC_FLR.1 | No Dependencies | |
| ALC_LCD.1 | No Dependencies | |
| ALC_TAT.2 | (ADV_IMP.1) | ADV_IMP.1 |
| ASE_CCL.1 | (ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1) | ASE_ECD.1, ASE_INT.1, ASE_REQ.2 |
| ASE_ECD.1 | No Dependencies | |
| ASE_INT.1 | No Dependencies | |
| ASE_OBJ.2 | (ASE_SPD.1) | ASE_SPD.1 |
| ASE_REQ.2 | (ASE_ECD.1) and (ASE_OBJ.2) | ASE_ECD.1, ASE_OBJ.2 |
| ASE_SPD.1 | No Dependencies | |
| ASE_TSS.1 | (ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1) | ADV_FSP.5, ASE_INT.1, ASE_REQ.2 |
| ATE_COV.2 | (ADV_FSP.2) and (ATE_FUN.1) | ADV_FSP.5, ATE_FUN.1 |
| ATE_DPT.3 | (ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1) | ADV_ARC.1, ADV_TDS.4, ATE_FUN.1 |

| | | |
|---|---|---|
| ATE_FUN.1 | (ATE_COV.1) | ATE_COV.2 |
| ATE_IND.2 | (ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1) | ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1 |
| AVA_VAN.5 | (ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1) | ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3 |

**Table 23 SARs Dependencies**

### *9.3.4 Rationale for the Security Assurance Requirements*

The EAL5 was chosen to permit a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

### *9.3.5 ALC_DVS.2 Sufficiency of security measures*

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

The component ALC_DVS.2 augmented to EAL5 has no dependencies to other security requirements.

### *9.3.6 AVA_VAN.5 Advanced methodical vulnerability analysis*

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

The component AVA_VAN.5 has the following dependencies:

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

All of these are met or exceeded in the EAL5 assurance package

### *9.3.7 ALC_FLR.1 Basic flaw remediation*

The flaw remediation assurance improves a rigourous management for updating the TOE in the context of sensible market.

# 10 TOE Summary Specification

## 10.1 TOE Summary Specification

**F.ACR - Access Control in Reading**

This function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor trying to access the data, and checks the access conditions are fulfilled as well as the life cycle state. It ensures that at any time, the following keys are never readable:

- Pre-personalization Agent keys,
- Personalization Agent keys,
- CA private key,
- Document basic access keys,
- Active Authentication Keys

Regarding the file structure:

*In the Operational Use phase*:

- The terminal can read user data, the Document Security Object, (EF.COM, EF.SOD, EF.DG1 to EF.DG16) only after EAC authentication and through a valid secure channel.

*In the Production and preparation stage*:

The Manufacturer can read the Initialization Data in Stage 2 "Production". The pre-personalization agent and the Personalization Agent can read only the random identifier in Stage 3 "Preparation" stored in the TOE. Other data-elements can only be read after they are authenticated by the TOE (using their authentication keys).

It ensures as well that no other part of the memory can be accessed at anytime

**F.ACW - Access Control in Writing**

This function controls access to write functions (in NVM) and enforces the security policy for data writing. Prior to any data update, it authenticates the actor, and checks the access conditions are fulfilled as well as the life cycle state.

Regarding the file structure:

*In the Operational Use phase*:

It is not possible to create any files (system or data files). Furthermore, it is not possible to update any files (system or data files), except for CVCA which can be updated if the "Secure Messaging" access condition is verified by the subjects defined in FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE..

*In the Production and preparation stage*:

The Manufacturer can write all the Initialization data and data for the Pre-personalization. The Personalization Agent can write through a valid secure channel all the data and Document Basic Access Keys, Chip Authentication Private Key, Active Authentication Keys and Country Verifying Certification Authority Public Key after it is authenticated by the TOE (using its authentication keys).

The Pre-Personalization Agent can write through a valid secure channel data to be used by the personalization agent (after it is authenticated by the TOE using its authentication

keys). The Pre-personalization agent is only active after delivery. The key that is written in the TOE for authentication purposes during manufacturing in meant for the pre-personalizaiton agent. the Pre-personalization agent (which is seen as a sub-role of thep Personalization agent) will refresh this key.

**F.AA - Active Authentication**

This security functionality ensures the Active Authentication is performed as described in [ICAO_9303] (if it is activated by the personalizer).

**F.CLR_INFO - Clear Residual Information**

This security function ensures clearing of sensitive information

- Authentication state is securely cleared in case an error is detected or a new authentication is attempted
- Authentication data related to GP authentication and EAC is securely cleared to prevent reuse
- Session keys is securely erased in case an error is detected or the secure communication session is closed

**F.CRYPTO - Cryptographic Support**

This Security Function provides the following cryptographic features:

- Key Generation based on ECDH with key sizes 192 to 512 bits.
- Key generation for Triple-DES in CBC mode for 112 bits.
- Key generation for AES in CBC mode with key sizes 128, 192 and 256 bits.
- Hashing using SHA-1 and SHA-256 meeting [FIPS_180_4]
- Secure messaging (encryption and decryption)using:
  - Triple-DES in CBC mode (keys size 112 bits)
  - AES in CBC mode (key sizes 128, 192 and 256 bits)
- Secure messaging (message authentication code) using:
  - Retail MAC with key size 112 bits
  - AES CMAC with key sizes 128, 192 and 256 bits
- Digital signature creation using:
  - ECDSA with SHA-1, SHA-256, SHA-384 and SHA-512 with key sizes 192 to 521 bits over prime field curves
  - RSA signature (CRT) with SHA-1, SHA-256, SHA-384 and SHA-512 with key sizes 1024, 1536, 2048, 3072 and 4096
- Digital signature verification using:
  - ECDSA with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 with key sizes 192 to 512 bits.
  - RSA PKCS#1v1.5 with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048, 3072 and 4096
  - RSA PKCS#1-PSS with SHA-1, SHA-256 and SHA-512 with key sizes 1024, 1536, 2048, 3072 and 4096
- GP Secure Messaging (encryption and decryption) using:
  - Triple-DES in CBC mode with key size 112 bits as defined in [FIPS_46_3].

- AES with key sizes 128, 192 and 256 bits as defined in [NIST_800_38A].

- GP Secure Messaging (message authentication code) using:
  - Retail MAC with key size 112 bits as defined in [ISO_9797_1].
  - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- Symmetric Authentication - encryption and decryption using:
  - Full 3DES MAC with key size 112 bits as defined in [ISO_9797_1].
  - AES CMAC with key sizes 128, 192 and 256 bits as defined in [NIST_800_38B].
- Key decryption using:
  - Triple-DES in ECB mode with key size 112 bits as defined in [FIPS_46_3].
  - AES in CBC mode with key sizes 128, 192 and 256 bits as defined in [FIPS_197].
- Chip Authentication Data Generation using DH, with key sizes 1024 to 2048 bits in steps of 512 bits.
- Chip Authentication Data Generation using ECDH, with key sizes 192 to 512 bits.
- Random number generation that meets the requirement the average Shannon entropy per internal random bit exceeds 0.994.

**F.EAC - Extended Access Control, EAC**

This TSF provides the Extended Access Control, authentication and session keys generation to be used by F.SM, as described in [TR_03110-3]. It also provides the following management functions:

- Maintain the roles: Document Verifier, CVCA, Domestic EIS, Foreign EIS
- Limit the ability to update the CVCA Public key and CVCA Certificate to the Country Verifying Certification Authority
- Limit the ability to update the date to CVCA, Document Verifier and Domestic Extended Inspection System.

**F.PERS - MRTD Personalization**

This security functionality ensures that the TOE, when delivered to the Personalization Agent, provides and requires authentication for data exchange. This authentication is based on a Triple DES and AES authentication mechanism. This security function is also responsible for management operations during personalization phase. This function allows to:

- Manage symmetric authentication using Personalization Agent keys,
- Configuration of the TOE
- Compute session keys to be used by F.SM,
- Load user data,
- Configure SM level for biometrical data access,
- Load Chip Authentication keys in encrypted form,
- Chip Authentication Key Generation,
- Write Active Authentication Keys,
- Enable and disable Active Authentication,
- Disable read access to Initialization Data,
- Write initial CVCA Public Key, initial CVCA Certificate and initial current date

- Write the document basic access keys,
- Set the files that are allowed to be modified in phase 7,
- Write the Document Security Object (SO d),
- Set TOE life cycle to Operational Use phase

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

**F.PHY - Physical Protection**

This Security Function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, configuration data and TOE life cycle. It detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

This Security Function also limits any physical emanations from the TOE so as to prevent any information leakge via these emanations that might reveal or provide access to sensitive data.

Furthermore, it prevents deploying test features after TOE delivery.

**F.PREP - MRTD Pre-personalization**

This security functionality ensures that the TOE, when delivered to the Manufacturer, provides and requires an authentication mechanism for data exchange. This authentication is based on Triple DES and AES symmetric authentication mechanism. This function allows to:

- Manage symmetric authentication using Pre-personalization Agent keys,
- Compute session keys to be used by F.SM,
- Initialization of the TOE,
- Load Personalization Agent keys in encrypted form,
- Store the Initialization and Pre-Personalization data in audit records.

In case the number of consecutive failed authentication attempts crosses 1 the TSF will slow down further authentication attempts.

**F.SM - Secure Messaging**

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Authentication Procedure (i.e. CA), a secure channel is established. This security functionality also provides a Secure Messaging (SCP02 and SCP03) for the transmission of user data in Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer or if the session is closed, the session keys are destroyed. This ensures protection against replay attacks as session keys are never reused.

**F.SS - Safe State Management**

This security functionality ensures that the TOE gets back to a secure state when:

- a tearing occurs (during a copy of data in NVM).
- an error due to self test as defined in FPT_TST.1.
- any physical tampering is detected.

This security functionality ensures that if such a case occurs, the TOE either is switched in the state "kill card" or becomes mute.

**F.STST - Self Test**

This security function implements self test features through platform functionalities at reset as defined in FPT_TST.1 to ensure the integrity of the TSF and TSF data.

**F.ADMIN - MRTD Administration**

This security functionality ensures that the TOE, when delivered to the Administration Agent, provides and requires authentication for data exchange. This function allows during Use phase to:

- Manage symmetric authentication using Administration Agent keys,
- Configure the size of the Chip Authentication key to be modified in USE phase,
- Change the CA key domain parameters used for the CA key generation process in user phase,
- Invalidate the primary Chip Authentication key in USE phase and to set the secondary key as being the primary key.

## 10.2 SFRs and TSS

### *10.2.1 SFRs and TSS - Rationale*

**Class FAU Security Audit**

**FAU_SAS.1** is met by F.PREP - MRTD Pre-personalization

**Class FCS Cryptographic Support**

**FCS_CKM.1/CA** is met by F.EAC - Extended Access Control, EAC that generates keys after a successful authentication using F.CRYPTO - Cryptographic Support

**FCS_CKM.4** is met by F.CLR_INFO - Clear Residual Information and F.SM - Secure Messaging that destroys the session keys upon closure of a secure messaging session.

**FCS_COP.1/SHA** is met by F.CRYPTO - Cryptographic Support.

**FCS_COP.1/SYM** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

**FCS_COP.1/MAC** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

**FCS_COP.1/SIG_VER** is met by F.EAC - Extended Access Control, EAC that uses F.CRYPTO - Cryptographic Support for Terminal Authentication.

**FCS_RND.1** is met by F.CRYPTO - Cryptographic Support

**Additional FCS SFR's Identified**

**FCS_CKM.1/CA_DATA_GEN** is met by F.PERS - MRTD Personalization that uses F.CRYPTO - Cryptographic Support to generate Chip Authentication Data.

**FCS_CKM.1/GP** is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that generate Cryptographic keys as defined in the requirement using F.CRYPTO - Cryptographic Support.

**FCS_COP.1/GP_ENC** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

**FCS_COP.1/GP_AUTH** is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Supportto perform Symmetric Authentication.

**FCS_COP.1/GP_MAC** is met by F.SM - Secure Messaging that uses F.CRYPTO - Cryptographic Support maintain a secure messaging session as defined in the requirement.

**FCS_COP.1/GP_KEY_DEC** is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that use F.CRYPTO - Cryptographic Support to perform key decryption.

**FCS_COP.1/AA** is covered by F.AA - Active Authentication in association with F.CRYPTO - Cryptographic Support

**Class FIA Identification and Authentication**

**FIA_UID.1** is met by F.ACR - Access Control in Reading that manages read access to data based on the current authentication state.

It is also met by F.EAC - Extended Access Control, EAC that allows Chip Authentication.

**FIA_UAU.1** is met by F.ACR - Access Control in Reading that manages read access to data based on the current authentication state.

It is also met by F.EAC - Extended Access Control, EAC that allows Chip Authentication.

**FIA_UAU.4** is met by F.CLR_INFO Clear Residual Information that ensures all authentication data is securely erased to prevent reuse.

**FIA_UAU.5/EAC** is met by F.EAC - Extended Access Control, EAC that provides Terminal Authentication.

SFR is also met by F.PERS - MRTD Personalization that provides symmetric authentication.

The SFR is also met by F.PREP - MRTD Pre-personalization that provides manufacturer authentication

Finally, it is also met by F.SM - Secure Messaging that provides a secure messaging session.

**FIA_UAU.6/EAC** is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

**FIA_API.1** is met by F.EAC - Extended Access Control, EAC that provides Chip Authentication as defined by [TR_03110-3]

**Additional FIA SFR's Identified**

**FIA_UID.1/MP** is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide semmetric authentication for manufacturer and personalization agent authentication.

**FIA_UAU.1/MP** is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that provide semmetric authentication for manufacturer and personalization agent authentication.

**FIA_UAU.6/MP** is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

**FIA_AFL.1/MP** is met by F.PREP - MRTD Pre-personalization and F.PERS - MRTD Personalization that ensure that after 3 authentication attempts the Toe increases time taken to respond to a terminal challenge.

**Class FDP User Data Protection**

**FDP_ACC.1** is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

**FDP_ACF.1** is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

**FDP_UCT.1/EAC** is met by F.SM - Secure Messaging that ensures all data is sent throught the secure communication channel after a successful Chip Authentication.

**FDP_UIT.1/EAC** is met by F.SM - Secure Messaging that ensures all messages are sent through the secure communication channel after Chip Authentication.

**Additional FDP SFR's Identified**

**FDP_ACC.1/UPD_FILE** is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

**FDP_ACF.1/UPD_FILE** is met by F.ACW - Access Control in Writing and F.ACR - Access Control in Reading that control read and write access to the data based on the current authentication state using authentication mechanisms provided by F.EAC - Extended Access Control, EAC and F.PERS - MRTD Personalization

**FDP_DAU.1/AA** is met by F.AA - Active Authentication that helps provide the gurantee of the TOE.

**FDP_ITC.1/AA** is met by F.ACW - Access Control in Writing that uses F.AA - Active Authentication to implement this access control policy.

**Class FMT Security Management**

**FMT_SMF.1** is met by F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization that utilizeF.ACW - Access Control in Writing to control write access via secure messaging provided by F.SM - Secure Messaging

**FMT_SMR.1** is met by F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization. These roles are maintained by means of the authentication states during the authentication mechanisms provided by the 3 Security Functions

**FMT_LIM.1** is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

**FMT_LIM.2** is met by F.PHY - Physical Protection and F.SS - Safe State Management that ensure that no data can be manipulated or revealed and the TSF assumes a safe state in case any illegal attempts to do so are detected.

**FMT_MTD.1/INI_ENA** is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

**FMT_MTD.1/INI_DIS** is met by F.PERS - MRTD Personalization that allows the personalization agent to disable read access in F.ACR - Access Control in Reading

**FMT_MTD.1/CVCA_INI** is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

**FMT_MTD.1/CVCA_UPD** is met by F.ACW - Access Control in Writing that controls access to updation of CVCA data by authentication through F.EAC - Extended Access Control, EAC

**FMT_MTD.1/DATE** is met by F.ACW - Access Control in Writing that controls access to updation of CVCA data by authentication through F.EAC - Extended Access Control, EAC

**FMT_MTD.1/KEY_WRITE** is met by F.PREP - MRTD Pre-personalization

**FMT_MTD.1/CAPK** is met by F.ACW - Access Control in Writing that ensures access conditions are met by way of authentication through F.PREP - MRTD Pre-personalization

**FMT_MTD.1/KEY_READ** is met by F.ACR - Access Control in Reading that ensures the secret keys are never readable.

**FMT_MTD.3** is met by F.EAC - Extended Access Control, EAC

**Additional FMT SFR's Identified**

**FMT_MOF.1/AA** is met by F.PERS - MRTD Personalization

**FMT_MOF.1/GP** is met by F.SM - Secure Messaging that provides a secure meants of transfer of user data after authentication using F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization

**FMT_MTD.1/LCS_PERS** is met by F.PERS - MRTD Personalization that allows the personalization agent after succesful authentication to switch the lifecycle state from phase 6 to phase 7

**FMT_MTD.1/UPD_FILE** is met by F.PERS - MRTD Personalization that controls access conditions in F.ACW - Access Control in Writing to allow only the name set by the personalization agent to be able to edit files in Operation Phase

**FMT_MTD.1/SM_LVL_DG3_DG4** is met by F.PERS - MRTD Personalisation that allows the personalisation agent to provide configure the secure messaging level required to access DG.3 and DG.4

**FMT_MTD.1/SM_LVL** is met by F.PERS - MRTD Personalisation in which the level of security of the allowed secure messaging can now be restricted during perso for the USE phase.

**FMT_MTD.1/AA_KEY_READ** is met by F.ACR - Access Control in Reading that ensures that Active Authentication Keys are never readable.

**FMT_MTD.1/AA_KEY_WRITE** is met by F.ACW - Access Control in Writing that uses F.PERS - MRTD Personalization to ensure Personalization Agent access is provided after successful authentication.

**FMT_MTD.1/ADMIN** is met by F.ADMIN - MRTD Administration, that ensures that the TOE, when delivered to the Administration Agent, provides and requires authentication for data exchange. This function allows during Use phase to:

- Manage symmetric authentication using Administration Agent keys,
- Modify the Chip Authentication key parameters to be used during key generation in USE phase,
- Change the key parameters during the key generation process,

- Invalidate one of the Chip Authentication key in USE phase and to set the secondary key as being the primary key.

**FMT_MTD.1/Key_Usage_Counter** is met by F.PERS - MRTD Personalisation that allows the personalisation agent to configure a Key Usage Counter that is decremented by one each time the key is used. Once the counter is depleted, the key becomes unusable. In the case of CA key, the Key Usage Counter will be reset to the maximum usage if the CA key is re-generated in USE phase. This Key Usage Counter is an optional parameter during the creation of the key in PERSO phase and if not configured, the usage of the key will be unlimited.

**Class FPT Protection of the Security Functions**

**FPT_EMS.1** is met by F.PHY - Physical Protection that prevents emanations beyond permissible limits to prevent any accidental revelation of data.

**FPT_FLS.1** is met by F.SS - Safe State Management.

**FPT_TST.1** is met by F.STST - Self Test that performs self tests to ensure integrity of the TSF

**FPT_PHP.3** is met by F.PHY - Physical Protection that protects the TOE against any physical probing or tampering by using F.SS - Safe State Management in case any physical manipulation is detected.

**Class FTP Trusted path/channels**

**FTP_ITC.1/MP** is met by F.SM - Secure Messaging that provides a ssecure channel for communication after authentication as defined in F.PERS - MRTD Personalization and F.PREP - MRTD Pre-personalization

### *10.2.2 Association tables of SFRs and TSS*

| Security Functional Requirements | TOE Summary Specification |
|---|---|
| FAU_SAS.1 | F.PREP - MRTD Pre-personalization |
| FCS_CKM.1/CA | F.EAC - Extended Access Control, EAC, F.CRYPTO - Cryptographic Support |
| FCS_CKM.4 | F.SM - Secure Messaging, F.CLR_INFO - Clear Residual Information |
| FCS_COP.1/SHA | F.CRYPTO - Cryptographic Support |
| FCS_COP.1/SYM | F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/MAC | F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/SIG_VER | F.EAC - Extended Access Control, EAC, F.CRYPTO - Cryptographic Support |

| | |
|---|---|
| FCS_RND.1 | F.CRYPTO - Cryptographic Support |
| FCS_CKM.1/CA_DATA_GEN | F.CRYPTO - Cryptographic Support, F.PERS - MRTD Personalization |
| FCS_CKM.1/GP | F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/GP_ENC | F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/GP_AUTH | F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/GP_MAC | F.SM - Secure Messaging, F.CRYPTO - Cryptographic Support |
| FCS_COP.1/GP_KEY_DEC | F.CRYPTO - Cryptographic Support, F.PREP - MRTD Pre-personalization, F.PERS - MRTD Personalization |
| FCS_COP.1/AA | F.AA - Active Authentication, F.CRYPTO - Cryptographic Support |
| FIA_UID.1 | F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC |
| FIA_UAU.1 | F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC |
| FIA_UAU.4 | F.CLR_INFO - Clear Residual Information |
| FIA_UAU.5/EAC | F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization, F.SM - Secure Messaging, F.PREP - MRTD Pre-personalization |
| FIA_UAU.6/EAC | F.SM - Secure Messaging |
| FIA_API.1 | F.EAC - Extended Access Control, EAC |
| FIA_UID.1/MP | F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |
| FIA_UAU.1/MP | F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |
| FIA_UAU.6/MP | F.SM - Secure Messaging |
| FIA_AFL.1/MP | F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |
| FDP_ACC.1 | F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization |
| FDP_ACF.1 | F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization |
| FDP_UCT.1/EAC | F.SM - Secure Messaging |

| | |
|---|---|
| FDP_UIT.1/EAC | F.SM - Secure Messaging |
| FDP_ACC.1/UPD_FILE | F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization |
| FDP_ACF.1/UPD_FILE | F.ACW - Access Control in Writing, F.ACR - Access Control in Reading, F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization |
| FDP_DAU.1/AA | F.AA - Active Authentication |
| FDP_ITC.1/AA | F.ACW - Access Control in Writing, F.AA - Active Authentication |
| FMT_SMF.1 | F.ACW - Access Control in Writing, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization, F.SM - Secure Messaging |
| FMT_SMR.1 | F.EAC - Extended Access Control, EAC, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |
| FMT_LIM.1 | F.SS - Safe State Management, F.PHY - Physical Protection |
| FMT_LIM.2 | F.PHY - Physical Protection, F.SS - Safe State Management |
| FMT_MTD.1/INI_ENA | F.ACW - Access Control in Writing, F.PREP - MRTD Pre-personalization |
| FMT_MTD.1/INI_DIS | F.ACR - Access Control in Reading, F.PERS - MRTD Personalization |
| FMT_MTD.1/CVCA_INI | F.ACW - Access Control in Writing, F.PERS - MRTD Personalization |
| FMT_MTD.1/CVCA_UPD | F.ACW - Access Control in Writing, F.EAC - Extended Access Control, EAC |
| FMT_MTD.1/DATE | F.ACW - Access Control in Writing, F.EAC - Extended Access Control, EAC |
| FMT_MTD.1/KEY_WRITE | F.PERS - MRTD Personalization |
| FMT_MTD.1/CAPK | F.ACW - Access Control in Writing, F.PERS - MRTD Personalization |
| FMT_MTD.1/KEY_READ | F.ACR - Access Control in Reading |
| FMT_MTD.3 | F.EAC - Extended Access Control, EAC |
| FMT_MOF.1/AA | F.PERS - MRTD Personalization |
| FMT_MOF.1/GP | F.SM - Secure Messaging, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |
| FMT_MTD.1/LCS_PERS | F.PERS - MRTD Personalization |
| FMT_MTD.1/UPD_FILE | F.ACW - Access Control in Writing, F.PERS - MRTD Personalization |

| | |
|---|---|
| FMT_MTD.1/SM_LVL_DG3_DG4 | F.PERS - MRTD Personalization |
| FMT_MTD.1/SM_LVL | F.PERS - MRTD Personalization |
| FMT_MTD.1/AA_KEY_READ | F.ACR - Access Control in Reading |
| FMT_MTD.1/AA_KEY_WRITE | F.ACW - Access Control in Writing, F.PERS - MRTD Personalization |
| FMT_MTD.1/ADMIN | F.ADMIN - MRTD Administration |
| FMT_MTD.1/Key_Usage_Counter | F.PERS - MRTD Personalization |
| FPT_EMS.1 | F.PHY - Physical Protection |
| FPT_FLS.1 | F.SS - Safe State Management |
| FPT_TST.1 | F.STST - Self Test |
| FPT_PHP.3 | F.PHY - Physical Protection, F.SS - Safe State Management |
| FTP_ITC.1/MP | F.SM - Secure Messaging, F.PERS - MRTD Personalization, F.PREP - MRTD Pre-personalization |

**Table 24 SFRs and TSS - Coverage**

| TOE Summary Specification | Security Functional Requirements |
|---|---|
| F.ACR - Access Control in Reading | FIA_UID.1, FIA_UAU.1, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_MTD.1/INI_DIS, FMT_MTD.1/KEY_READ, FMT_MTD.1/AA_KEY_READ |
| F.ACW - Access Control in Writing | FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FDP_ITC.1/AA, FMT_SMF.1, FMT_MTD.1/INI_ENA, FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.1/CAPK, FMT_MTD.1/UPD_FILE, FMT_MTD.1/AA_KEY_WRITE |
| F.AA - Active Authentication | FCS_COP.1/AA, FDP_DAU.1/AA, FDP_ITC.1/AA |
| F.CLR_INFO - Clear Residual Information | FCS_CKM.4, FIA_UAU.4 |
| F.CRYPTO - Cryptographic Support | FCS_CKM.1/CA, FCS_COP.1/SHA, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/SIG_VER, FCS_RND.1, FCS_CKM.1/CA_DATA_GEN, FCS_CKM.1/GP, FCS_COP.1/GP_ENC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_MAC, FCS_COP.1/GP_KEY_DEC, FCS_COP.1/AA |
| F.EAC - Extended Access Control, EAC | FCS_CKM.1/CA, FCS_COP.1/SIG_VER, FIA_UID.1, FIA_UAU.1, FIA_UAU.5/EAC, FIA_API.1, FDP_ACC.1, FDP_ACF.1, FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_SMR.1, FMT_MTD.1/CVCA_UPD, FMT_MTD.1/DATE, FMT_MTD.3 |
| F.PERS - MRTD Personalization | FCS_CKM.1/CA_DATA_GEN, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FIA_UAU.5/EAC, FIA_UID.1/MP, FIA_UAU.1/MP, FIA_AFL.1/MP, FDP_ACC.1, FDP_ACF.1, |

| | |
|---|---|
| | FDP_ACC.1/UPD_FILE, FDP_ACF.1/UPD_FILE, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_DIS, FMT_MTD.1/CVCA_INI, FMT_MTD.1/KEY_WRITE, FMT_MTD.1/CAPK, FMT_MOF.1/AA, FMT_MOF.1/GP, FMT_MTD.1/LCS_PERS, FMT_MTD.1/UPD_FILE, FMT_MTD.1/SM_LVL_DG3_DG4, FMT_MTD.1/SM_LVL, FMT_MTD.1/AA_KEY_WRITE, FMT_MTD.1/Key_Usage_Counter, FTP_ITC.1/MP |
| F.PHY - Physical Protection | FMT_LIM.1, FMT_LIM.2, FPT_EMS.1, FPT_PHP.3 |
| F.PREP - MRTD Pre-personalization | FAU_SAS.1, FCS_CKM.1/GP, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FIA_UAU.5/EAC, FIA_UID.1/MP, FIA_UAU.1/MP, FIA_AFL.1/MP, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1/INI_ENA, FMT_MOF.1/GP, FTP_ITC.1/MP |
| F.SM - Secure Messaging | FCS_CKM.4, FCS_COP.1/SYM, FCS_COP.1/MAC, FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FIA_UAU.5/EAC, FIA_UAU.6/EAC, FIA_UAU.6/MP, FDP_UCT.1/EAC, FDP_UIT.1/EAC, FMT_SMF.1, FMT_MOF.1/GP, FTP_ITC.1/MP |
| F.SS - Safe State Management | FMT_LIM.1, FMT_LIM.2, FPT_FLS.1, FPT_PHP.3 |
| F.STST - Self Test | FPT_TST.1 |
| F.ADMIN - MRTD Administration | FMT_MTD.1/ADMIN |

**Table 25 TSS and SFRs - Coverage**